cellebrite
delivering mobile expertise

UFED series

UFED Physical Analyzer

Manuel de l'utilisateur

Décembre 2014

Avis juridiques

Copyright © 2014 Cellebrite Mobile Synchronization Ltd. Tous droits réservés.

Ce manuel fourni est sujet aux conditions et restrictions suivantes :

- Ce manuel contient des informations propriétaires appartenant à Cellebrite Mobile Synchronization Ltd. De telles informations sont fournies uniquement dans le but d'assigner explicitement et correctement les utilisateurs autorisés au UFED Physical Analyzer.
- Aucune partie de ce contenu ne peut être utilisée à d'autres fins, dévoilée à toute personne ou société, ou reproduite de toute manière, électronique ou mécanique, sans l'autorisation expresse préalable et écrite de Cellebrite Ltd.
- Les textes et graphiques sont donnés dans un but d'illustration et de référence seulement. Les spécifications sur lesquelles ils sont basés sont sujettes à modification sans préavis.
- Les informations contenues dans ce document sont sujettes à modification sans préavis. Les noms et données d'entreprise et de personnes utilisés ici dans des exemples sont fictifs sauf mention contraire.

Contenu

Chapitre 1 : Introduction 11

1.1. Présentation 11

1.2. Extraction physique 12

1.3. Analyse de données 14

Chapitre 2 : Installation et activation 17

2.1. Installer UFED Physical Analyzer 18

2.1.1. Configuration requise 18

2.1.2. Installation du logiciel 19

2.1.3. Activer UFED Physical Analyzer 27

2.1.4. Déplacer UFED Physical Analyzer vers un autre PC à l'aide d'une licence logicielle 35

2.1.5. Permettre la connectivité avec Windows Vista 37

Chapitre 3 : Mise en route 39

3.1. Lancer UFED Physical Analyzer 40

3.2. Démonstration de Link Analysis 40

3.3. Ouvrir une extraction pour analyse 41

3.4. Ouvrir une extraction en mode avancé 44

3.4.1. Ouverture avancée d'un fichier d'extraction UFED 44

3.4.2. Ouverture avancée d'un fichier d'extraction non-UFED 57

3.4.3. Enregistrement d'un fichier .ufd 69

3.5. Enregistrer une session de projet 70

3.6. Charger une session de projet 71

3.7. Fermer un projet 72

3.8. Fermer UFED Physical Analyzer 72

3.9. Raccourcis clavier 73

Chapitre 4 : S'orienter dans l'espace de travail 75

4.1. Arborescence de projet.....76
4.1.1. Travailler dans la zone Arborescence de projet.....89
4.2. Zone d'affichage de données.....90
4.2.1. Onglet Accueil.....92
4.2.2. Onglet Résumé d'extraction.....94
4.2.3. Onglets de données.....96

Chapitre 5 : Localisation et analyse des informations..... 119

5.1. Rechercher des informations dans un onglet de données.....119
5.2. Utiliser le filtre rapide.....119
5.3. Utiliser le filtre avancé.....122
5.4. Rechercher des informations dans tous les projets ouverts.....123
5.5. Parcourir le système de fichiers.....124
5.6. Vue Chronologie.....126
5.7. Accéder à la vue Conversation.....129
5.8. Travailler avec les listes de surveillance.....132
5.8.1. Créer une liste de surveillance.....132
5.8.2. Modifier une liste de surveillance.....137
5.8.3. Importer une liste de surveillance.....137
5.8.4. Exporter une liste de surveillance.....140
5.8.5. Supprimer une liste de surveillance.....142
5.8.6. Exécuter une liste de surveillance.....142
5.8.7. Localiser une liste de surveillance.....145
5.9. Informations sur les signets (signets d'entités).....145
5.9.1. Créer un nouveau signet d'entité.....147
5.9.2. Modifier un signet d'entité.....148
5.9.3. Supprimer un signet d'entité.....148
5.10. Localisation des appareils.....149
5.10.1. À propos des données de localisation.....149
5.10.2. Afficher les données de localisation sur BING.....152

5.10.3. Indicateurs et fenêtres d'informations....155
5.10.4. Récupération des adresses....156

Chapitre 6 : Traduction de données décodées....159

6.1. Utilisation de la fonction....160

6.2. Mettre à jour votre licence avec les langues sélectionnées....160

6.2.1. Sélectionner des langues dans MyCellebrite....160
6.2.2. Téléchargez le package de traduction....166
6.2.3. Traduction de données décodées....168
6.2.4. Reporting....170

Chapitre 7 : Travailler avec l'analyse de projet....173

Chapitre 8 : Rechercher les malware....177

8.1. Mettre à jour la base de données de signature (en ligne)....178

8.2. Mettre à jour la base de données de signature depuis un fichier (hors connexion)....180

Chapitre 9 : Générer un rapport....187

Chapitre 10 : Effectuer des extractions...199

10.1. Extraction d'appareils iOS....199
10.1.1. Conditions préalables....199
10.1.2. Effectuer une extraction physique....200
10.1.3. Effectuer une extraction numérique avancée....216

10.2. Extraction du GPS ou des appareils de stockage de masse....227
10.2.1. Lire des données depuis un appareil GPS ou de stockage de masse....230

Chapitre 11 : Paramètres avancés....235

11.1. Travailler avec TomTom....235
11.1.1. Exporter un fichier TomTom....236
11.1.2. Importer un fichier TomTom....237

11.2. Reconstituer des images....239
11.2.1. Rechercher les images reconstituées....240
11.2.2. Travailler avec les images reconstituées 243
11.3. Vérifier les valeurs de hachage....244

Chapitre 12 : Travailler avec les données hexadécimales 247

12.1. Rechercher des informations dans les données hexadécimales et dans les données décodées....250
12.1.1. Rechercher des chaînes....252
12.1.2. Rechercher des octets....257
12.1.3. Rechercher des dates....262
12.1.4. Rechercher des numéros SIM ICCID....268
12.1.5. Rechercher des numéros SMS....273
12.1.6. Rechercher des expressions régulières (GREP)....279
12.1.7. Rechercher des chaînes de texte de SMS....285
12.1.8. Rechercher des schémas....291
12.1.9. Rechercher des codes et des mots de passe....297
12.2. Parcourir l'extraction hexadécimale....302
12.3. Utiliser un décalage pour accéder directement à un emplacement différent dans le fichier....303
12.4. Travailler avec les signets....304
12.4.1. Ajouter un signet....304
12.4.2. Modifier un signet....307
12.4.3. Supprimer un signet....307
12.5. Décoder des données brutes....308
12.6. Afficher les informations des données hexadécimales....310
12.7. Localiser des types de données spécifiques dans les données hexadécimales....311

Chapitre 13 : Preuve appareil photo et capture d'écran 313

Chapitre 14 : Décodage avancé 317

14.1. Gérer les chaînes 317
14.1.1. Construire une chaîne 319
14.1.2. Modifier une chaîne existante 321
14.1.3. Gérer les chaînes d'appareils 324
14.1.4. Supprimer une chaîne 330
14.1.5. Description des chaînes 330
14.2. Plug-ins 334
14.2.1. Gérer les plug-ins 335
14.2.2. Exécuter un plug-in spécifique 337
14.3. Utiliser le shell Python 339
14.4. Exporter le système de fichiers 340
14.5. Utiliser le plug-in de reconstitution de schéma de déverrouillage Android 340
14.6. Plug-in de reconstitution de mot de passe de déverrouillage Android 341

Chapitre 15 : Paramètres 343

15.1. Paramètres généraux 344
15.2. Fichiers de données 347
15.2.1. Méthodes de filtrage des fichiers de données 348
15.2.2. Gérer les paramètres des fichiers de données 349
15.3. Paramètres de la visionneuse hexadécimale 353
15.4. Paramètres des modèles 355
15.5. Champs de rapport supplémentaires 356
15.5.1. Ajouter un champ de rapport 357
15.5.2. Modifier un champ de rapport 359
15.5.3. Supprimer un champ de rapport 359
15.6. Paramètres par défaut du rapport 359
15.7. Paramètres de plug-in post-chaîne 370
15.8. Enregistrer les paramètres 371
15.9. Charger des paramètres 372

15.10. Définir les paramètres du projet....372
15.10.1. Définir un fuseau horaire unifié pour le projet....372
15.10.2. Définir les informations du dossier....376

Chapitre 16 : Références 379

16.1. Menu Fichier....379
16.2. Menu Vue....380
16.2.1. Afficher la fenêtre Trace....380
16.3. Menu Outils....382
16.4. Menu Extraction....384
16.5. Menu Python....384
16.6. Menu Plug-ins....385
16.7. Menu Rapport....385
16.8. Menu Aide....386

Chapitre 1 : **Introduction**

1.1. Présentation

UFED est divisé en trois composants :

- L'unité UFED Touch ou UFED permet l'extraction numérique, de mot de passe, de SIM, de système de fichiers et physique d'appareils mobiles. L'extraction peut ensuite être enregistrée sur une clé USB, une carte mémoire SD ou directement sur votre PC.
- L'application UFED Physical Analyzer offre une vision en profondeur de la mémoire de l'appareil, à l'aide de méthodes avancées de décodage, d'analyse et de création de rapports. UFED Physical Analyzer peut décoder tous les types d'extractions créés par l'unité UFED Touch ou UFED Classic.
- L'application Phone Detective permet aux investigateurs d'identifier rapidement un téléphone mobile en fonction de ses attributs physiques, sans avoir besoin d'allumer l'appareil et de risquer son verrouillage.

UFED fonctionne en deux étapes :

- Extraction : extraction physique, de système de fichiers, numérique, de mot de passe, de carte SIM à l'aide de l'unité UFED Touch ou UFED.

- Le décodage, l'analyse et la génération de rapports sont effectués à l'aide de UFED Physical Analyzer.

1.2. Extraction physique

Au cours d'une extraction physique, UFED utilise des méthodes d'extraction avancées pour créer un fichier d'extraction hexadécimal unique pour chaque puce de mémoire flash ou plage d'adressage utilisé par l'appareil mobile. Contrairement aux processus d'extraction numérique, la méthode d'extraction physique contourne le système d'exploitation de l'appareil et extrait les données directement de la mémoire flash interne de l'appareil. La mémoire de l'appareil est capturée sous forme de fichiers d'extraction hexadécimaux qui peuvent ensuite être lus et décodés à l'aide de UFED Physical Analyzer.

L'extraction physique ainsi créée inclut l'espace mémoire non attribué par le système d'exploitation de l'appareil, qui peut contenir des données supprimées, notamment SMS, journaux d'appel, entrées de carnet d'adresses, images, vidéos et mots de passe utilisateur.

L'extraction physique permet de faire une copie bit par bit de la totalité de la mémoire Flash d'un appareil mobile. Le décodage des extractions physiques permet non seulement d'acquérir des données intactes, mais aussi des données masquées ou supprimées. Les données supprimées peuvent être récupérées dans les fichiers et l'espace libre[1].

[1] L'espace libre est composé de grappes de partitions multimédia non utilisées pour stocker des fichiers actifs. Il peut contenir des fragments de fichiers supprimés de la partition de fichier, mais non supprimés du disque physique.

UFED Physical Analyzer offre des algorithmes de reconstitution avancés, en récupérant les enregistrements SQLite pour révéler des données supprimées supplémentaires de l'espace libre. La quantité de données supprimées varie en fonction des données présentes sur l'appareil. Les données décodées sont affichées dans les mêmes listes que les données analysées. Par exemple, les SMS supprimés de l'espace libre sont affichés dans la même liste que les SMS.

La reconstitution des données de l'espace libre offre les avantages suivants :

- Solution la plus rapide et la plus efficace du marché pour récupérer les données supprimées.
- Davantage de données supprimées, plus rapidement.
- Révèle des données supprimées qui n'étaient pas disponibles auparavant.
- Meilleure qualité des données car les faux positifs et les doublons sont automatiquement supprimés.
- Activation automatique : Aucune activation manuelle n'est nécessaire.
- Prend en charge plusieurs types de contenu, tels que : SMS, MMS, appels, contacts, e-mails et données des applications[2].
- Même vue : Possibilité d'organiser l'ensemble des données, y compris les données décodées à partir de l'espace libre, dans les mêmes vues et avec des chronologies.

[2] Données d'applications telles que : Kik, WhatsApp, Facebook, Facebook Messenger, Twitter, etc.

1.3. Analyse de données

UFED Physical Analyzer permet à l'investigateur d'effectuer une analyse en profondeur des données extraites et de générer des rapports.

UFED Physical Analyzer présente les caractéristiques principales suivantes :

- Décodage de l'extraction avec une vue stratifiée du contenu de la mémoire :
    - Offre une vue détaillée du fichier hexadécimal.
    - Reconstruit le système de fichiers de l'appareil.
    - Décode plusieurs types de données analysées, notamment : liste de contacts, SMS, journaux d'appel, informations de l'appareil (IMSI, ICCID, codes utilisateur), informations sur l'application, etc. ;
    - Offre une vue des fichiers de données : images, vidéos, bases de données, etc.
    - Permet d'accéder aux donnes existantes et supprimées.
    - Révèle les mots de passe de l'appareil (le cas échéant).
- Extraction puissante pour les appareils iOS et GPS.
- Offre une interface utilisateur intuitive et conviviale pour parcourir les informations extraites.
- Outils d'analyse et de recherche puissants :
    - Recherche instantanée de tout le contenu du projet.
    - Recherche avancée selon plusieurs paramètres.
    - Recherche instantanée du contenu des tableaux de données.

    - Liste de surveillance pour mettre en évidence les informations en fonction d'une liste de valeurs prédéfinies.
    - Chronologie pour consulter tous les événements effectués via l'appareil mobile sur une seule vue chronologique.
    - Analyse de projets pour une analyse complète de l'activité.
    - Scanner anti-malware pour identifier les malware présents dans l'appareil.
    - Capacité à effectuer une recherche hexadécimale selon plusieurs paramètres (chaînes, octets, chiffres, dates).
    - Capacité à utiliser une recherche d'expression régulière (RegEx) pour rechercher des chaînes de données spécifiques.
- Capacité à ajouter des signets à différents emplacements de la mémoire pour indexer les zones importantes afin de les étudier ultérieurement.
- Capacité à utiliser les commandes shell Python pour l'analyse des données.
- Plug-ins :
    - Ajouter ou supprimer des plug-ins.
    - Écrivez vos propres plug-ins à l'aide du langage script Python.
    - Gérer les chaînes.
- Rapports :
    - Créez des rapports dans plusieurs formats.
    - Personnalisation des rapports (logo, en-tête, etc.).

Chapitre 2 : **Installation et activation**

Ce chapitre décrit le processus d'installation et d'activation de UFED Physical Analyzer sur votre PC.

2.1. Installer UFED Physical Analyzer

2.1.1. Configuration requise

PC	PC compatible avec Windows, avec processeur Pentium® IV ou compatible, fonctionnant à 1,6 GHz ou plus
Système d'exploitation	Microsoft Windows XP[3] avec SP3 ou plus récent Microsoft Windows Vista™, Windows 7 ou Windows 8
Mémoire (RAM)	Système d'exploitation — Recommandé — Minimum 32 bits — 4 Go — 4 Go 64 bits — 8 Go — 4 Go
Espace requis	500 Mo d'espace libre sur le disque pour l'installation
Conditions supplémentaires	Microsoft® .Net version 4.0 REMARQUE : Windows XP 64 bits nécessite l'installation d'un correctif .Net 2.0 (NDP20-KB913384-X64.exe), téléchargeable à l'adresse http://archive.msdn.microsoft.com/KB913384/Release/ProjectReleases.aspx?ReleaseId=771

[3] À compter du 28 février 2015, la série UFED ne prendra plus en charge Windows XP.

Autorisations	Si vous avez l'intention d'activer l'application à l'aide d'une clé de licence logicielle (dongle) fournie par Cellebrite, vous devez disposer de droits d'administrateurs sur l'ordinateur.

REMARQUE : Pour permettre l'extraction vers un PC avec le système d'exploitation Windows Vista, suivez la procédure décrite dans la section ***Permettre la connectivité avec Windows Vista*** (page ***37***).

2.1.2. Installation du logiciel

2.1.2.1. Obtenir une copie de UFED Physical Analyzer

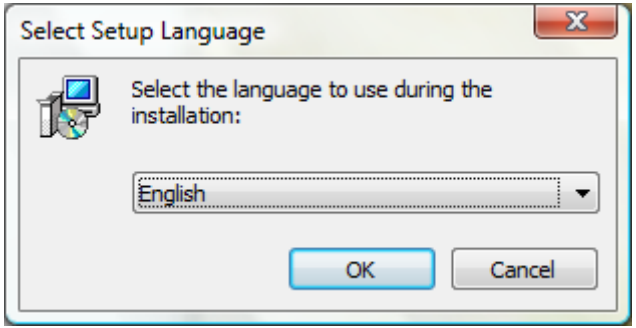
Vous pouvez trouver une copie du logiciel d'installation le plus récent pour l'application UFED Physical Analyzer auprès des sources suivantes :

- CD UFED Physical Analyzer.
- En le téléchargeant sur le site MyCellebrite.
- En le téléchargeant à l'aide du lien fourni dans les notes de publication.

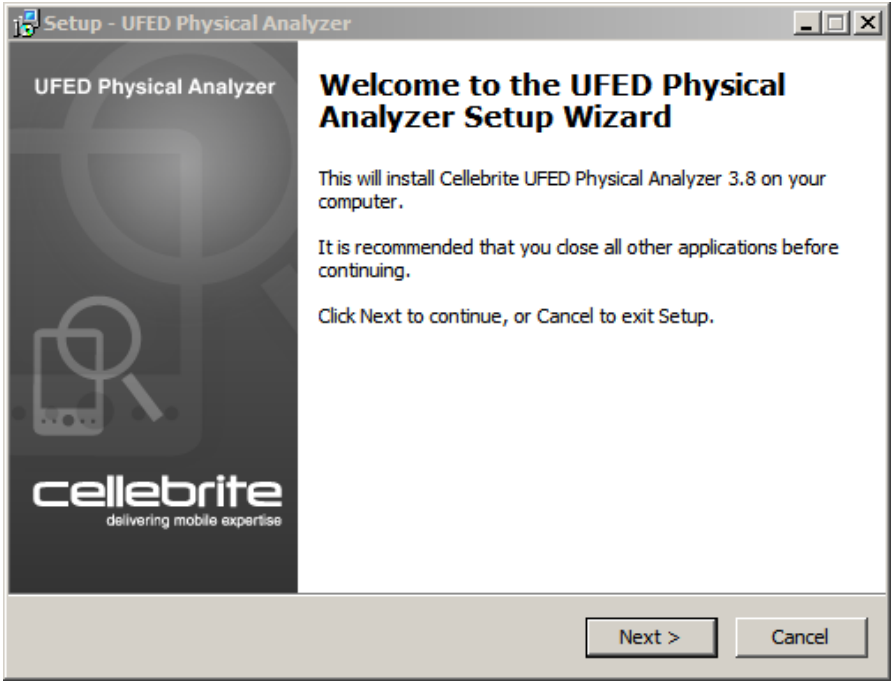
2.1.2.2. Installer UFED Physical Analyzer

REMARQUE : Avant de commencer, assurez-vous qu'aucun câble U-441 n'est branché à votre ordinateur.

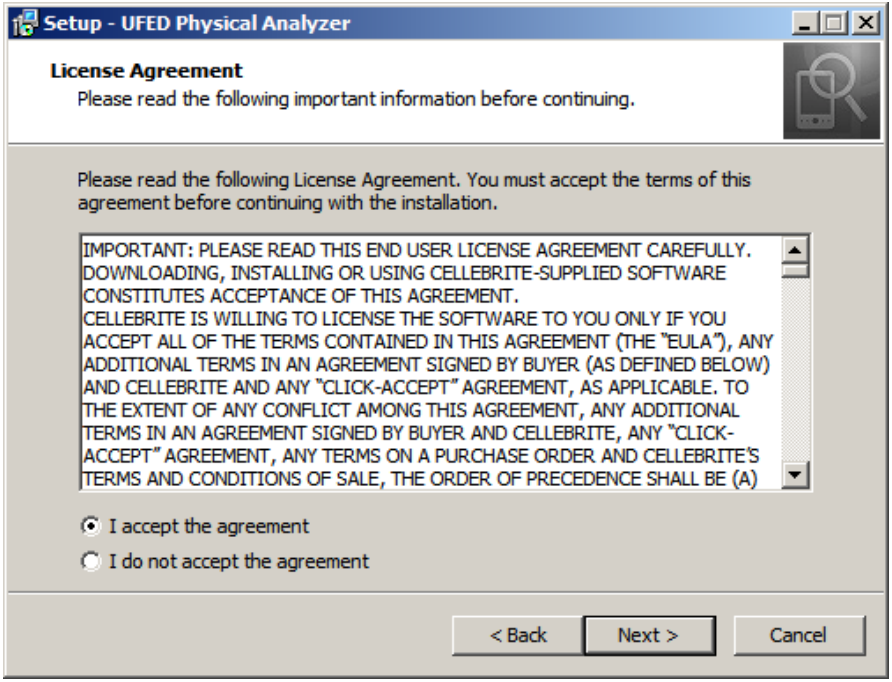
1) Double-cliquez sur le fichier de configuration.



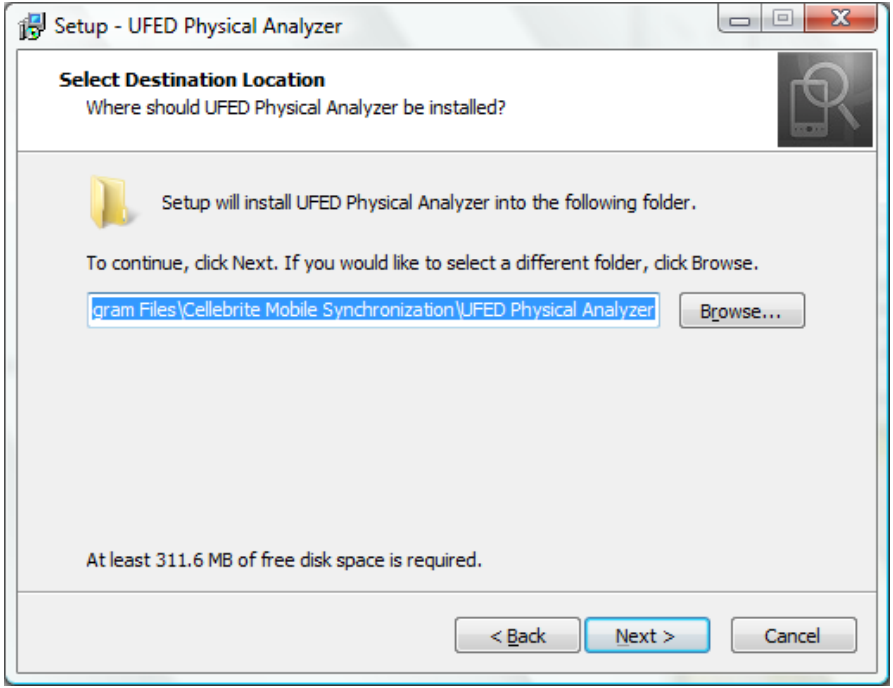
2) Sélectionnez la langue de votre choix, puis cliquez sur **OK** pour continuer.


Setup - UFED Physical Analyzer
UFED Physical Analyzer
Welcome to the UFED Physical Analyzer Setup Wizard
This will install Cellebrite UFED Physical Analyzer 3.8 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
cellebrite
delivering mobile expertise
Next >
Cancel

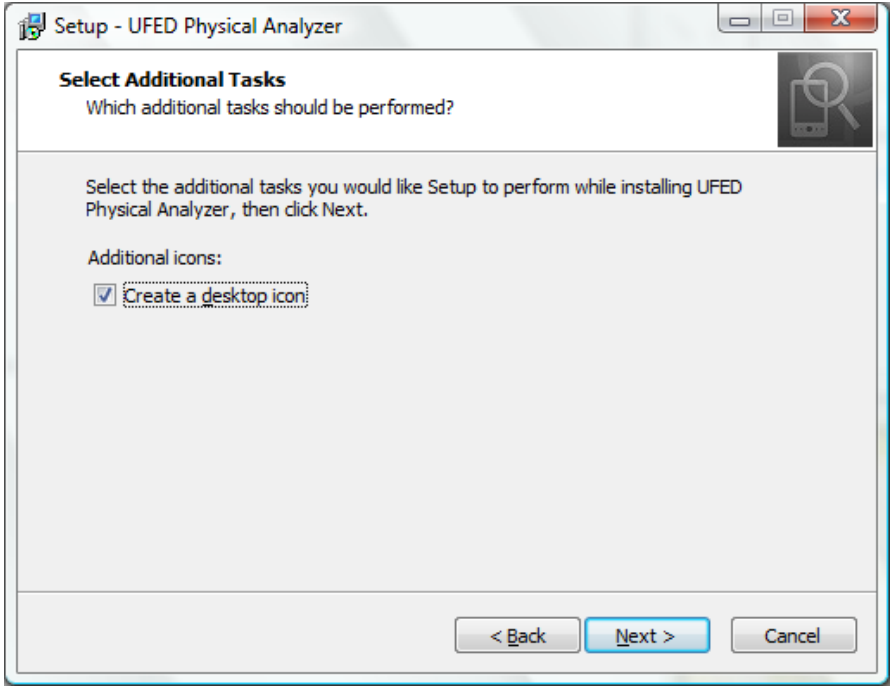
3) Cliquez sur **Suivant**.


Setup - UFED Physical Analyzer
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CELLEBRITE-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CELLEBRITE IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS AGREEMENT (THE "EULA"), ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER (AS DEFINED BELOW) AND CELLEBRITE AND ANY "CLICK-ACCEPT" AGREEMENT, AS APPLICABLE. TO THE EXTENT OF ANY CONFLICT AMONG THIS AGREEMENT, ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE, ANY "CLICK-ACCEPT" AGREEMENT, ANY TERMS ON A PURCHASE ORDER AND CELLEBRITE'S TERMS AND CONDITIONS OF SALE, THE ORDER OF PRECEDENCE SHALL BE (A)
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

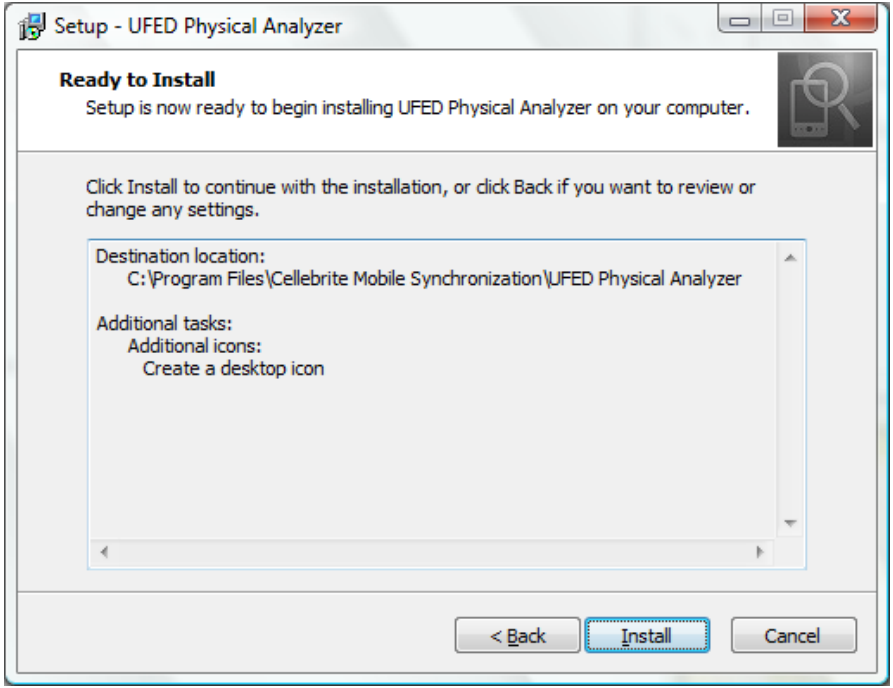
4) Sélectionnez **J'accepte l'accord**, puis cliquez sur **Suivant**.


Setup - UFED Physical Analyzer
Select Destination Location
Where should UFED Physical Analyzer be installed?
Setup will install UFED Physical Analyzer into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
gram Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer
Browse...
At least 311.6 MB of free disk space is required.
< Back
Next >
Cancel

5) Si vous le souhaitez, cliquez sur **Parcourir** pour choisir un dossier d'installation différent.
6) Cliquez sur **Suivant**.


Setup - UFED Physical Analyzer
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing UFED Physical Analyzer, then click Next.
Additional icons:
Create a desktop icon
< Back
Next >
Cancel

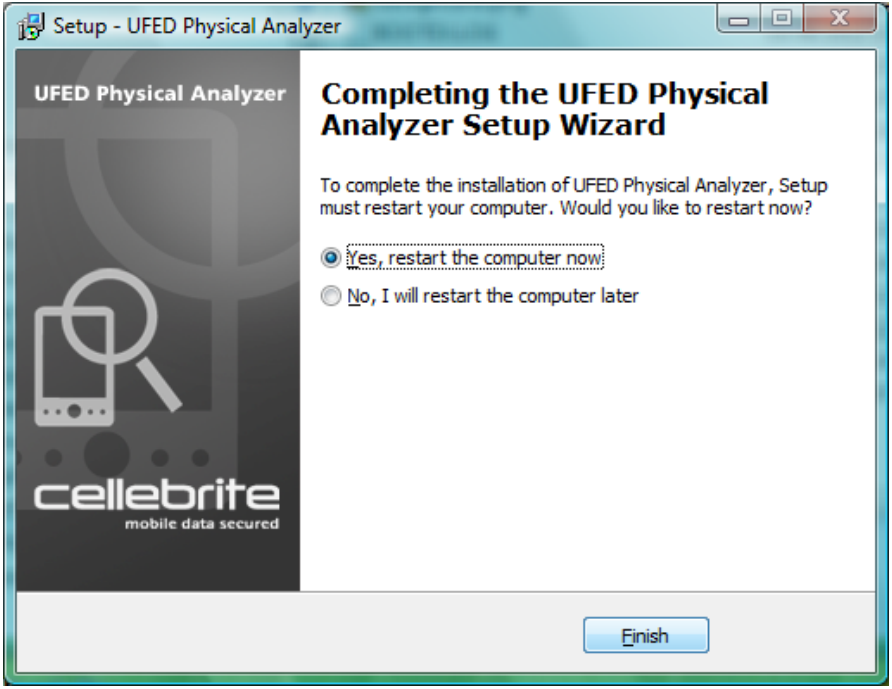
7) Si vous ne souhaitez pas qu'une icône soit placée sur le bureau, décochez la case **Créer une icône sur le bureau**.
8) Cliquez sur **Suivant**.


Setup - UFED Physical Analyzer
Ready to Install
Setup is now ready to begin installing UFED Physical Analyzer on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer
Additional tasks:
Additional icons:
Create a desktop icon
< Back
Install
Cancel

9) Cliquez sur **Installer**.

L'installation commence.

REMARQUE : Dans le cadre du processus d'installation, il peut vous être demandé de télécharger et d'installer Microsoft .NET 3.5 Framework. Un accès à Internet depuis votre ordinateur est nécessaire pour effectuer cette étape de l'installation.


Setup - UFED Physical Analyzer
UFED Physical Analyzer
cellebrite
mobile data secured
Completing the UFED Physical Analyzer Setup Wizard
To complete the installation of UFED Physical Analyzer, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
Finish

10) Sélectionnez **Redémarrer maintenant**, puis cliquez sur **Terminer**.

Votre ordinateur redémarre, et UFED Physical Analyzer est installé.

2.1.3. Activer UFED Physical Analyzer

Pour activer UFED Physical Analyzer, utilisez une des méthodes suivantes :

- Utiliser une clé de licence (dongle)
- Utiliser une licence logicielle
- Utiliser une clé réseau (dongle)

REMARQUE : Consultez votre kit UFED pour vérifier quelle méthode vous devez utiliser.

2.1.3.1. Notification de nouvelle version

Cellebrite vous informe lorsqu'une nouvelle version de votre logiciel est disponible. Si vous êtes connecté à Internet, vous recevrez cette notification lorsque la nouvelle version est disponible. Si vous n'êtes pas connecté à Internet, cette notification s'affiche tous les 3 mois.

Clé de licence (dongle) UFED

2.1.3.2. Utiliser une clé de licence (dongle)

Utilisez le dongle UFED fourni dans votre kit UFED. Le dongle contient les licences de toutes les applications achetées.

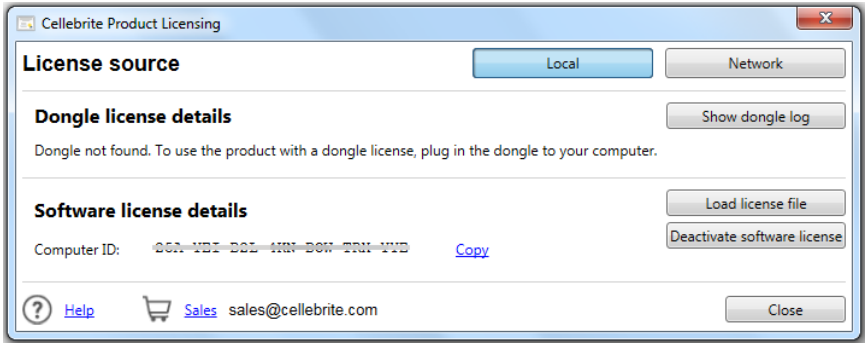
Pour utiliser UFED Physical Analyzer avec un dongle :

1) Connectez le dongle à un port USB de votre ordinateur. La licence est automatiquement détectée. Une fois le dongle reconnu par le système d'exploitation, l'application peut lire la licence.
2) Lancez UFED Physical Analyzer.

Félicitations ! Votre application est maintenant prête à l'emploi.

Si la clé de licence (dongle) est introuvable :

1) Lorsque vous le lancez pour la première fois, ou lorsqu'une clé de licence est introuvable, la fenêtre « Licence du produit Cellebrite » s'affiche.



2) Si vous avez connecté le dongle à un port USB sur votre ordinateur, et qu'il ne fonctionne toujours pas, contactez-nous à l'adresse support@cellebrite.com.

REMARQUE : Les pilotes du dongle HASP doivent être installés pour pouvoir utiliser une clé de licence matérielle. Si les pilotes n'ont pas été installés lors du processus d'installation du logiciel UFED, vous pouvez exécuter le processus d'installation à nouveau, et sélectionner Installer les pilotes du dongle Hasp à la fin du processus.

2.1.3.3. Utilisation de l'application avec une clé logicielle

Vous devez activer la licence lors du premier démarrage de l'application.

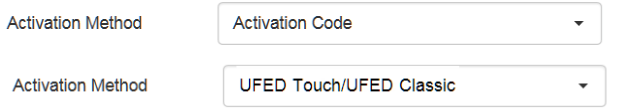
Pour utiliser UFED Physical Analyzer avec une licence logicielle :

1) Cliquez sur le lien suivant : https://my.cellebrite.com/physicalanalyzer
2) Connectez-vous à votre compte MyCellebrite.

   (Si vous ne possédez pas de compte, cliquez sur **Inscrivez-vous maintenant**, créez un utilisateur, puis retournez au lien vers l'application UFED souhaitée.)

   Vous êtes alors dirigé sur la fenêtre d'activation du produit.
3) Cliquez sur Télécharger l'application et enregistrez le fichier sur le PC.
4) Extrayez le fichier Zip, cliquez sur le fichier d'installation et installez le logiciel à l'aide de l'assistant d'installation. Redémarrez l'ordinateur si cela vous est demandé.
5) Répétez l'étape 1 pour accéder au lien vers l'application.

6) Dans la fenêtre Méthode d'activation, si vous avez acheté UFED 4PC, sélectionnez **Code d'activation** ou si vous avez acheté UFED Touch, sélectionnez **UFED Touch/UFED Classic**.

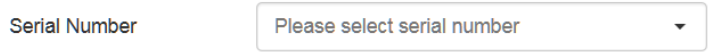


Code d'activation

7) Selon le produit que vous avez acheté, continuez de la façon suivante :

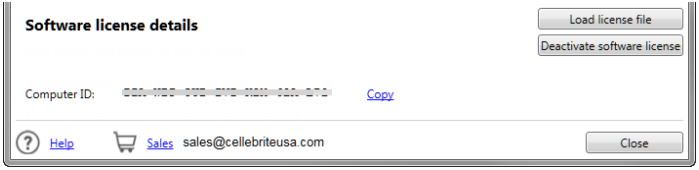
- **UFED 4PC :** Dans le champ Code d'activation, entrez le code d'activation fourni avec le kit UFED 4PC.

- **UFED Touch :** Dans le champ Choisir le numéro de série, sélectionnez le numéro de série UFED affiché sur l'unité UFED Touch ou sur l'écran Activation de la licence UFED Touch.



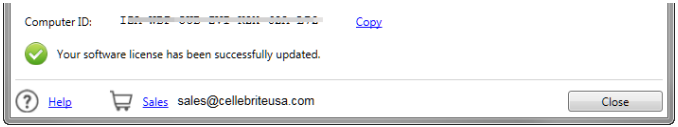
8) Récupérez ensuite l'ID ordinateur (ne fermez pas la page MyCellebrite lors de cette étape).

- Lancez l'application. La fenêtre « Licence de produit Cellebrite » s'affiche.
- Cliquez sur **Copier** pour copier l'ID ordinateur affiché à l'écran.



9) Sur MyCellebrite, collez l'ID ordinateur copié.

10) Cliquez sur **Télécharger maintenant !** pour télécharger la clé de licence de votre application sur votre PC. La clé de licence est également envoyée à votre adresse e-mail enregistrée sur MyCellebrite.
11) Dans l'application, cliquez sur **Charger le fichier de licence** dans la fenêtre Licence de produit Cellebrite.
12) Sélectionnez le fichier « License » et cliquez sur **Ouvrir**. Un message s'affiche pour vous indiquer que la licence logicielle a bien été mise à jour.



13) Cliquez sur **Fermer**.

Félicitations ! Votre application est maintenant prête à l'emploi.

2.1.3.4. Utiliser une clé réseau (dongle)

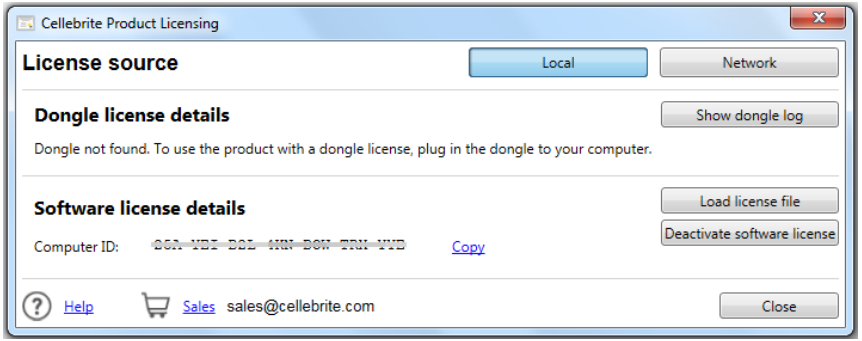
Clés réseau UFED

La clé réseau est connectée au réseau de votre entreprise et contient les licences de toutes les applications achetées.

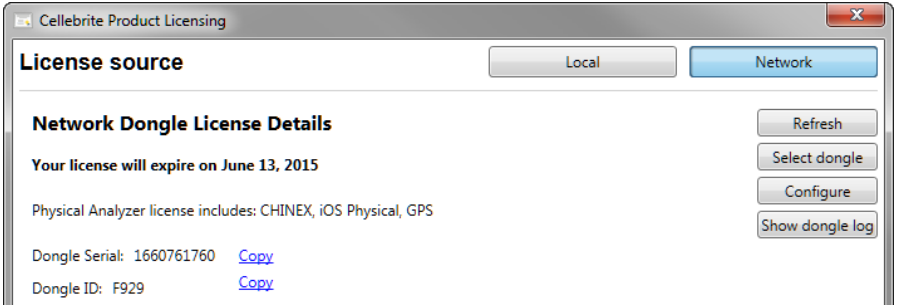
Pour utiliser UFED Physical Analyzer avec une clé réseau :

1) Lancez l'application UFED. Si la clé réseau est connectée au réseau, l'application démarre et l'utilisateur peut commencer à travailler immédiatement.

   Si la clé réseau n'est pas reconnue, la fenêtre « Licence de produit Cellebrite » s'affiche.



2) Cliquez sur **Réseau**. La fenêtre suivante s'affiche :



REMARQUE : Si aucune clé n'est trouvée sur le réseau, assurez-vous d'être connecté à Internet et qu'une clé est connectée au réseau. Cliquez ensuite sur **Rafraîchir** pour rechercher une clé réseau à nouveau.

REMARQUE : Par défaut, la configuration du réseau est Diffusion. Si nécessaire, vous pouvez connecter manuellement la clé réseau. Cliquez sur **Configurer** pour modifier la configuration du réseau et choisissez l'option Hôte spécifique. Saisissez le nom de l'hôte (ou son adresse IP) et le numéro de port (1 à 5 chiffres).

REMARQUE : Si une seule clé réseau est disponible, elle est sélectionnée automatiquement. S'il y a plusieurs clés réseau, sélectionnez la clé souhaitée dans la liste, puis cliquez sur **Appliquer**.

Félicitations ! Votre application est maintenant prête à l'emploi.

2.1.4. Déplacer UFED Physical Analyzer vers un autre PC à l'aide d'une licence logicielle

Lorsqu'une installation de UFED Physical Analyzer activée par une licence logicielle doit être déplacée vers un autre PC, vous devez d'abord désactiver (supprimer) la licence de l'ordinateur d'origine. Le processus de désactivation varie selon les versions de la licence. Suivez les instructions fournies par votre application.

2.1.4.1. Désactivation des licences de la version 2

1) Dans UFED Physical Analyzer, allez dans **Aide** > **Afficher les détails de la licence**.

   La fenêtre « Licence de produit Cellebrite » s'affiche.

2) Cliquez sur **Désactiver la licence logicielle**.

   La fenêtre « Désactivation de la licence logicielle » s'affiche.

3) Cliquez sur **Générer le fichier de désactivation**.

   UFED Physical Analyzer est désactivé.

4) Pour obtenir votre nouvelle licence UFED Physical Analyzer, rendez-vous à l'adresse **http://my.cellebrite.com/physicalanalyzer**, et suivez les étapes d'activation de la licence. Pour plus d'informations, consultez la section ***Activation à l'aide d'une licence logicielle*** (page ***30***).

2.1.4.2. Désactivation des licences de la version 5

1) Dans UFED Physical Analyzer, allez dans **Aide** > **Afficher les détails de la licence**.

   La fenêtre « Désactivation de la licence logicielle » s'affiche.

2) Cliquez sur **Désactiver la licence logicielle**.

   La fenêtre « Désactivation de la licence logicielle » s'affiche.

3) Cliquez sur **Copier** pour copier l'identifiant de l'ordinateur.
4) Rendez-vous sur la page **http://my.cellebrite.com/deactivation**, et connectez-vous à votre compte MyCellebrite.

   Si vous n'avez pas de compte, cliquez sur **Inscription** et créez un utilisateur. Puis revenez à la page http://my.cellebrite.com/deactivation.

   Vous êtes alors dirigé vers l'assistant de désactivation.

5) Collez l'identifiant de l'ordinateur, puis cliquez sur **Suivant**.
6) Cliquez sur **Télécharger** et téléchargez le fichier de désactivation sur le PC.
7) Dans UFED Physical Analyzer, allez dans **Aide** > **Afficher les détails de la licence**.
8) Cliquez sur **Sélectionner le fichier de désactivation**, puis sélectionnez le fichier de désactivation sélectionné à l'étape 6.

   Votre licence est désactivée, et UFED Physical Analyzer créez un fichier de désactivation. La fenêtre « Désactivation de la licence logicielle » vous informe que le fichier de désactivation a été créé.

9) Revenez à l'assistant de désactivation dans MyCellebrite.
10) Cliquez sur **Choisir le fichier**, puis téléchargez le fichier de désactivation créé par UFED Physical Analyzer.
11) Cliquez sur **Terminer**.
12) Pour obtenir votre nouvelle licence UFED Physical Analyzer, rendez-vous à l'adresse **http://my.cellebrite.com/physicalanalyzer**, et suivez les étapes d'activation de la licence. Pour plus d'informations, consultez la section ***Activation à l'aide d'une licence logicielle*** (page ***30***).

2.1.5. Permettre la connectivité avec Windows Vista

Suivez la procédure ci-dessous pour permettre à l'unité UFED de se connecter aux ordinateurs sur lesquels le système d'exploitation Windows Vista est installé.

1) Accédez au dossier Cellebrite Physical Analyzer **Drivers\cbrtucbl**.
2) Double-cliquez sur **USB_Cable_DRV.exe**.
3) Suivez les instructions à l'écran.

Chapitre 3 : **Mise en route**

UFED Physical Analyzer propose des outils de décodage et d'analyse puissants pour les données extraites d'un appareil, et simplifie la tâche de navigation au sein des structures de données de l'appareil. UFED Physical Analyzer vous assiste dans l'exécution de tâches complexes telles que la collecte d'informations, la recherche d'investigation et la création de rapports constituant des preuves légales.

Cette application est conçue pour utiliser la mémoire extraite par l'unité UFED et présente l'extraction hexadécimale, le système de fichiers et les données analysées de l'appareil sous forme claire et concise, permettant aux investigateurs d'utiliser des outils de recherche puissants pour découvrir des informations pertinentes.

Enfin, une dernière étape vous permet de créer des rapports dans plusieurs formats, tels que HTML, PDF, Excel (*.xlsx) et XML.

3.1. Lancer UFED Physical Analyzer

Pour lancer UFED Physical Analyzer, utilisez une des méthodes suivantes :

- Double-cliquez sur le raccourci bureau de **UFED Physical Analyzer**.
- Sélectionnez **Démarrer > Programmes > Cellebrite Mobile Synchronization > UFED Physical Analyzer**.

  Pour une présentation de l'espace de travail, consultez la section ***S'orienter dans l'espace de travail*** (page ***75***).

3.2. Démonstration de Link Analysis

Lorsque vous ouvrez UFED Physical Analyzer, il vous est proposé d'afficher un exemple de projet dans **UFED Link Analysis**.

La démonstration UFED Link Analysis contient un exemple de contenu préchargé. Ce contenu ce compose de 3 rapports avec des exemples d'images, SMS, MMS et de nombreuses autres informations. Les 3 personnes chargées sont connectées les unes aux autres de différentes façons.

La démonstration a défini certains détails relatifs aux personnes, filtres de données, a ouvert l'onglet Carte et créé une chronologie. Tout cela compose un projet Link Analysis simple.

3.3. Ouvrir une extraction pour analyse

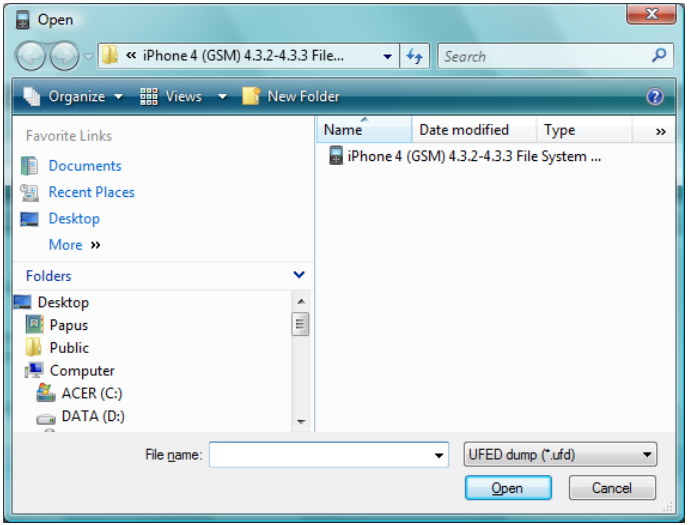
UFED Physical Analyzer permet d'ouvrir les fichiers créés par l'appareil UFED, les fichiers XML créés par UFED Physical Analyzer, les fichiers UFDR, les fichiers UFD et les fichiers URP (ces fichiers sont créés dans l'application UFED Report Manager). En mode avancé, UFED Physical Analyzer peut ouvrir les fichiers images. Pour plus d'informations, consultez la section ***Ouvrir une extraction en mode avancé*** (page ***44***).

1) Si les données de l'appareil ont été extraites vers un disque amovible, connectez la clé USB ou la carte SD contenant les données extraites à votre PC.

   REMARQUE : Pour accélérer le traitement, copiez le dossier d'extraction du disque amovible vers le PC.

2) Utilisez une des méthodes suivantes :
   - Dans l'onglet **Accueil**, cliquez sur **Ouvrir**.
   - Glissez-déposez le fichier UFD dans UFED Physical Analyzer.
   - Dans la barre d'outils de l'application, cliquez sur .

- Dans le menu de l'application, sélectionnez **Fichier** > **Ouvrir**.



3) Accédez au dossier dans lequel se trouvent les données extraites de l'appareil, et ouvrez-le.
4) Sélectionnez une extraction dans l'un des formats pris en charge suivants :
    - Fichier de vidage UFED (*.ufd).
    - Fichiers binaires (*.bin). Fichiez binaires bruts ou toute extraction hexadécimale générée par une autre application à l'aide de la fonctionnalité d'ouverture avancée. Voir ***Ouvrir une extraction en mode avancé*** (page ***44***).

- Nokia PM (*.pm) ;
- Fichier de sauvegarde BlackBerry (*.ipd) ;
- Fichier de sauvegarde BlackBerry (*.bbb) ;
- Sony Ericsson GDFS (*.gdfs, *.bin) ;
- TomTom CFG (*.cfg) ;
- Rapport UFED (*.xml) – Rapports numériques générés par l'unité UFED et rapports XML créés par UFED Physical Analyzer ;
- UFED Report Manager (*.urp, *.ucp) – rapports du package de rapports UFED/Pack de contenu UFED créés par Report Manager ;
- Package de rapport UFED (*.ufdr).

REMARQUE : Par défaut, la boîte de dialogue « Ouvrir » est configurée pour afficher le fichier *ufd, qui est le fichier de mappage des informations des données extraites de l'appareil.

5) Cliquez sur **Ouvrir**.

Le processus d'analyse des données (y compris l'analyse du projet) commence. Cela peut durer plusieurs minutes. À la fin du processus, un nouveau projet est ajouté à l'arborescence de projet, et le **Résumé d'extraction** apparaît dans la zone d'affichage des données.

REMARQUE : Pour ouvrir une extraction rapidement lorsque UFED Physical Analyzer est fermé, double-cliquez sur le fichier *.ufd dans le répertoire d'extraction. UFED Physical Analyzer s'ouvre et commence l'analyse des données.

3.4. Ouvrir une extraction en mode avancé

La fonctionnalité Ouvrir (avancé) vous permet de spécifier les options de l'extraction de données de l'appareil et de décodage.

Choisissez parmi deux méthodes d'ouverture de projet principales :

- **Sélectionner une extraction UFED** : vous permet de spécifier comment décoder un fichier d'extraction UFED (*.ufd).
- **Commencer sans fichier .ufd** : vous permet de commencer à décoder une extraction physique ou un système de fichiers qui n'a pas été généré par une unité UFED.

3.4.1. Ouverture avancée d'un fichier d'extraction UFED

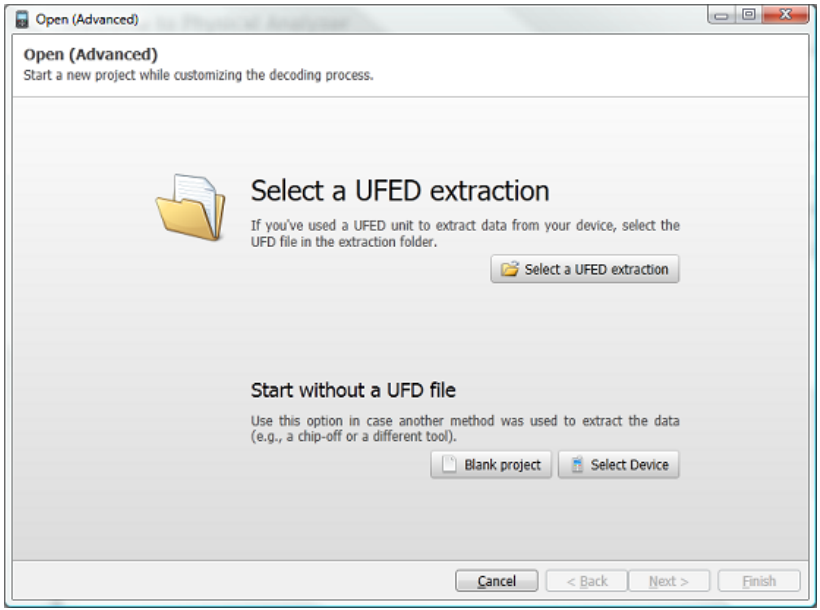
Le processus d'ouverture standard active un processus de décodage en fonction des informations relatives à l'appareil et au fabricant enregistrées sur le fichier *.ufd.

L'utilisation de la méthode **Sélectionner une extraction UFED** vous permet d'ignorer le processus d'ouverture standard et de spécifier un processus d'analyse personnalisé, ou de spécifier comment analyser les appareils inconnus.

Pour créer un nouveau projet à partir des données extraites par UFED avec l'option Ouvrir (avancé) :

1) Sélectionnez **Fichier** > **Ouvrir (avancé)** ou cliquez sur .

   La boîte de dialogue Ouvrir (avancé) s'affiche, vous permettant de définir le processus de décodage des données extraites pour votre nouveau projet.


Open (Advanced)
Open (Advanced)
Start a new project while customizing the decoding process.
Select a UFED extraction
If you've used a UFED unit to extract data from your device, select the UFD file in the extraction folder.
Select a UFED extraction
Start without a UFD file
Use this option in case another method was used to extract the data (e.g., a chip-off or a different tool).
Blank project
Select Device
Cancel
< Back
Next >
Finish

2) Cliquez sur **Sélectionner une extraction UFED**.
3) Dans la boîte de dialogue « Ouvrir », sélectionnez le fichier *.ufd à traiter, puis cliquez sur **OK**.

   Le contenu de la boîte de dialogue devient « Personnalisation avancée » et affiche les informations détectées suivantes en fonction du fichier *.ufd choisi :

   - **Appareil** - Nom du fabricant et modèle de l'appareil.
   - **Chaîne sélectionnée** - Chaîne de décodage standard de l'appareil automatiquement attribuée à l'appareil.
   - **Vidages binaires** - Images d'extraction binaires référencées par le fichier *.ufd.

4) Personnalisez les options d'ouverture du fichier en suivant la méthode décrite dans les sections suivantes.
5) Cliquez sur **Terminer**.

3.4.1.1. Spécifier un appareil différent

Vous pouvez spécifier un processus de décodage totalement différent pour l'extraction en remplaçant l'appareil sélectionné.

1) Cliquez sur **Changer d'appareil**.

2) Dans la liste **Sélectionner l'appareil**, sélectionnez l'appareil souhaité.
3) Pour filtrer les appareils affichés, procédez d'une des façons suivantes :
    - Cliquez sur le fabricant de l'appareil dans la liste de fabricants située sur le panneau de gauche.
    - Saisissez le nom de fabricant ou le modèle de l'appareil dans le champ **Filtre rapide** pour filtrer les appareils affichés.
4) Cliquez sur **Suivant** pour revenir à l'écran Personnalisation avancée.

3.4.1.2. Modifier la chaîne de décodage

Une chaîne est un ensemble de plug-ins regroupés dans un certain ordre et utilisé pour décoder les données extraites. Chaque appareil de la liste des appareils pris en charge par l'application dispose d'une chaîne de décodage prédéfinie.

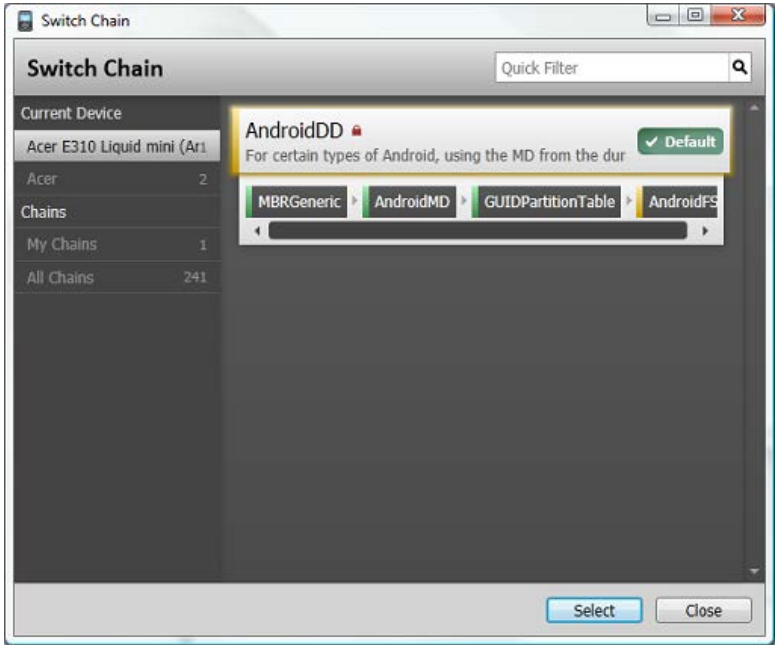
REMARQUE : Outre des plug-ins, une chaîne peut également contenir d'autres chaînes. C'est une façon simplifiée d'utiliser un ensemble de plug-ins prédéfinis dans une autre chaîne.

Pour en savoir plus sur les chaînes de décodage et les plug-ins, consultez les sections ***Décodage avancé*** (page ***317***) et ***Plug-ins*** (page ***334***).

Pour sélectionner une chaîne différente :

1) Cliquez sur **Changer de chaîne**.

   La fenêtre de dialogue « Changer de chaîne » s'ouvre et affiche la chaîne par défaut attribuée à l'appareil.



REMARQUE : Plusieurs chaînes peuvent être attribuées à un appareil, mais une seule est la chaîne par défaut.

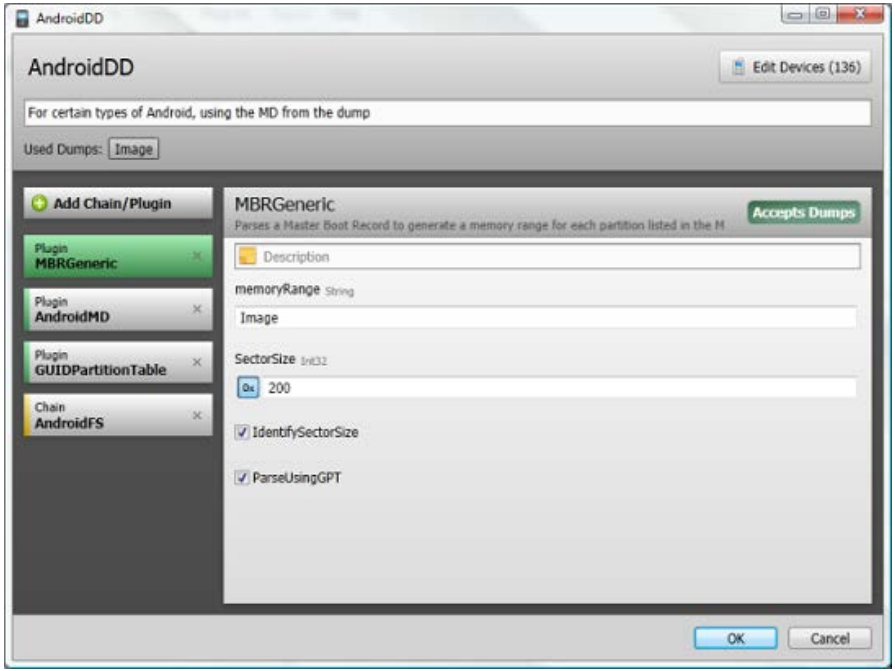
2) Dans la liste de chaînes, sélectionnez celle que vous souhaitez utiliser d'une des façons suivantes :
   - Sélectionnez le nom du fabricant dans la section **Appareil actuel** pour afficher les chaînes attribuées aux appareils du même fabricant.
   - Dans la section **Chaînes** de la liste :
     - Sélectionnez **Mes chaînes** pour choisir dans la liste de chaînes personnalisées que vous avez créée.
     - Sélectionnez **Toutes les chaînes** pour choisir dans la liste de toutes les chaînes prédéfinies de l'appareil.
     - Utilisez le champ « Filtre rapide » pour filtrer les éléments de la liste affichée.
3) Sélectionnez la chaîne souhaitée, puis cliquez sur **Sélectionner** pour revenir à l'écran Personnalisation avancée.

   La chaîne par défaut est remplacée par la chaîne sélectionnée.

Pour modifier la chaîne actuelle :

1) Cliquez sur **Modifier**.

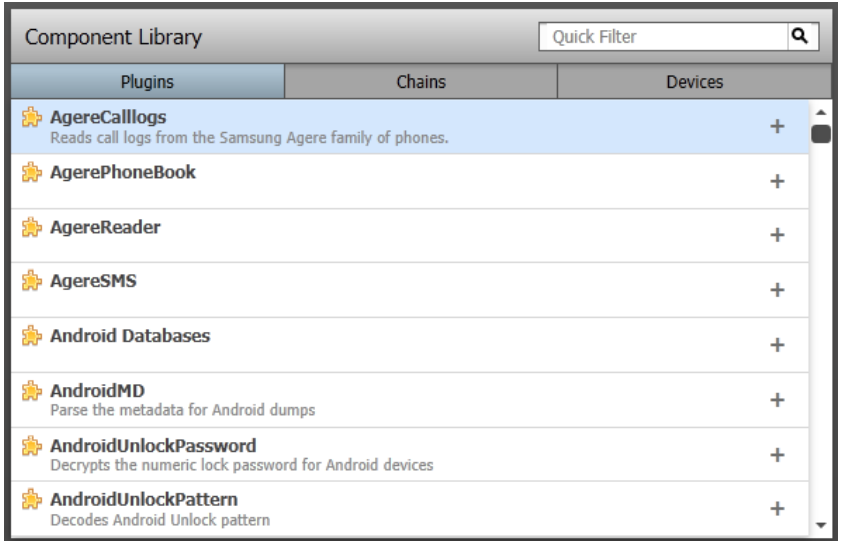
La boîte de dialogue Structure de la chaîne s'ouvre et affiche la chaîne.



2) Pour ajouter un composant à la chaîne :

   a) Cliquez sur **Ajouter une chaîne/un plug-in**.

   b) Dans la **Bibliothèque de composants**, sélectionnez un des éléments suivants :



- **Appareil** : chaîne complète d'un appareil spécifique.
- **Chaîne** : une chaîne prédéfinie spécifique.

- **Plug-in** : un plug-in spécifique.

REMARQUE : Un élément sélectionné sous **Appareil** ou **Chaîne** est ajouté à la chaîne comme **Composant de la chaîne**.

3) Cliquez sur + pour ajouter le composant.
4) Pour supprimer un composant de la liste de la chaîne, cliquez sur le « x » à droite du composant, puis sur **Oui** pour confirmer.
5) Cliquez sur **OK** pour revenir à l'écran de personnalisation avancée.

   La chaîne par défaut est remplacée par la chaîne personnalisée.

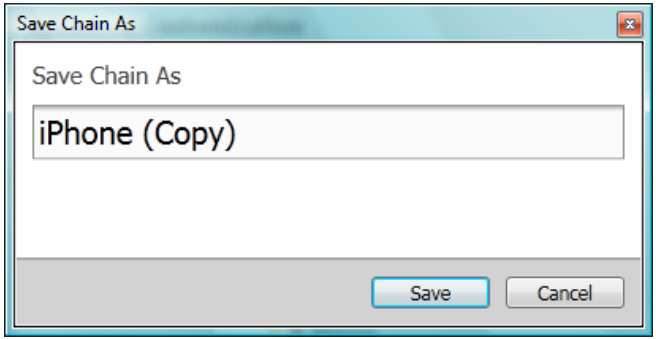
Pour enregistrer une chaîne personnalisée :

Après avoir personnalisé une chaîne, vous pouvez enregistrer les modifications apportées à celle-ci afin de la réutiliser ultérieurement à l'aide des boutons **Enregistrer sous** ou **Enregistrer** dans la section **Chaîne sélectionnée**.

REMARQUE : Le bouton **Enregistrer** est disponible uniquement pour les personnalisations de chaînes définies par l'utilisateur déverrouillées, enregistrées dans **Mes chaînes**. Pour en savoir plus sur les chaînes définies par l'utilisateur, consultez la section ***Gérer les chaînes*** (page ***317***).

1) Cliquez sur **Enregistrer** pour remplacer la chaîne définie par l'utilisateur par la chaîne actuelle, ou sur **Enregistrer sous** pour enregistrer la chaîne actuelle comme nouvelle chaîne.

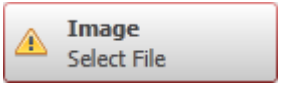
2) Si vous avez cliqué sur **Enregistrer sous**, saisissez un nom pour la nouvelle chaîne, puis cliquez sur **Enregistrer**.



La nouvelle chaîne est ajoutée à la liste de chaînes personnalisées **Mes chaînes** de l'application, et la chaîne enregistrée apparaît comme **Chaîne sélectionnée**.

3.4.1.3. Ajouter un vidage binaire

Vous pouvez ajouter des fichiers de vidage binaire reçus depuis une source différente.

- Pour ajouter un fichier de vidage binaire, cliquez sur 

ou **Ajouter un vidage binaire** dans la zone **Vidages binaires**, et sélectionnez le fichier d'extraction binaire que vous souhaitez ajouter. Chaque vidage binaire ajouté s'affiche comme composant distinct dans la section **Vidages binaires** de la boîte de dialogue.
- Pour supprimer un vidage binaire, cliquez sur , qui s'affiche lorsque vous placez le curseur de la souris sur celui-ci.

3.4.1.4. Ajouter un vidage de système de fichiers

Vous pouvez ajouter un vidage de système de fichiers au projet reçu sous forme d'archive ZIP ou de dossier contenant les fichiers d'extraction du système de fichiers.

- Pour ajouter une extraction de système de fichiers, cliquez sur **Fichier Zip** ou **Dossier,** puis sélectionnez l'archive ZIP ou le dossier que vous souhaitez ajouter.

  REMARQUE : Vous ne pouvez ajouter qu'une seule extraction de système de fichiers. Si vous tentez d'en ajouter plusieurs, le vidage de système de fichiers ajouté précédemment est supprimé, qu'il s'agisse d'une archive ZIP ou d'un dossier.

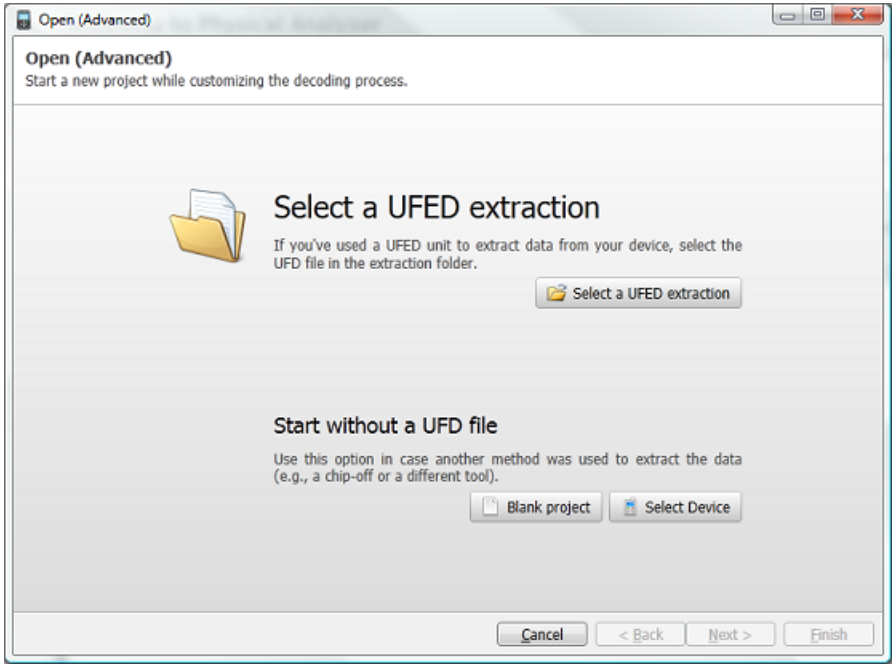
- Pour supprimer une extraction de système de fichiers, cliquez sur , qui s'affiche lorsque vous placez le curseur de la souris sur celui-ci.

3.4.2. Ouverture avancée d'un fichier d'extraction non-UFED

Lorsque vous recevez des extractions binaires ou de système de fichiers non générées par une unité UFED, ou si vous ne disposez pas du fichier *.ufd qui les accompagne, vous pouvez utiliser la fonctionnalité Ouvrir (avancé) pour définir comment les décoder pour le nouveau projet.

1) Sélectionnez **Fichier** > **Ouvrir (avancé)** ou cliquez sur .

La boîte de dialogue Ouvrir (avancé) s'affiche, vous permettant de définir le processus de décodage des données extraites pour votre nouveau projet.

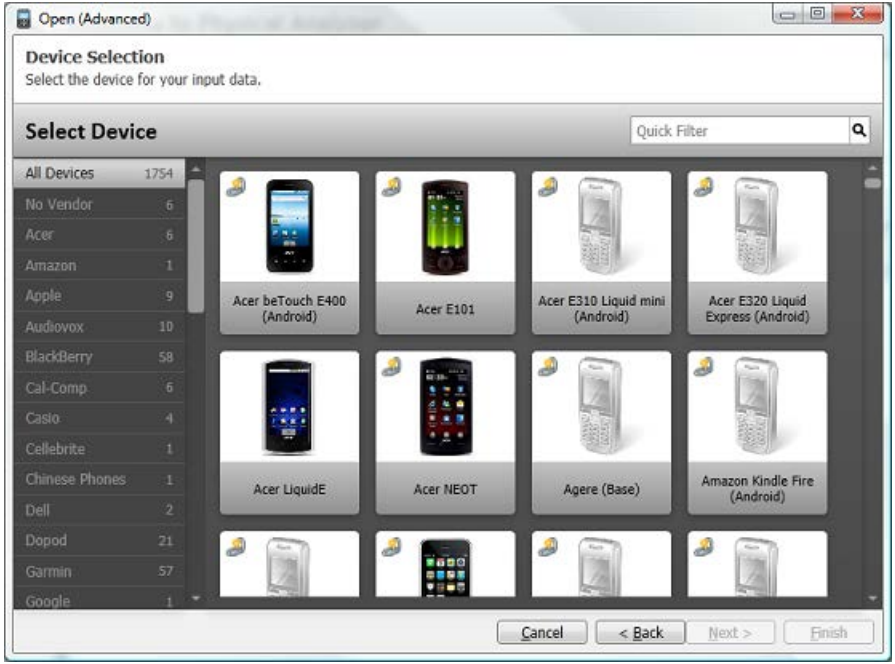

Open (Advanced)
Open (Advanced)
Start a new project while customizing the decoding process.
Select a UFED extraction
If you've used a UFED unit to extract data from your device, select the UFD file in the extraction folder.
Select a UFED extraction
Start without a UFD file
Use this option in case another method was used to extract the data (e.g., a chip-off or a different tool).
Blank project
Select Device
Cancel
< Back
Next >
Finish

2) En cliquant sur l'option **Commencer sans fichier UFD**, vous disposez de deux points de départ pour votre nouveau projet :
    - **Sélectionner l'appareil** - Sélectionnez la définition spécifique de l'appareil à utiliser pour décoder l'extraction de données. Cette option est utile lorsque vous connaissez le fabricant et le modèle de l'appareil. Consultez la section ***Commencer par la sélection de l'appareil*** (page ***59***).
    - **Nouveau projet** - Offre un panneau **Personnalisation avancée** vide vous permettant de définir les données et paramètres du processus. Cette option est utile lorsque vous n'avez aucune information sur l'appareil et/ou le fabricant, et souhaitez créer un processus de décodage personnalisé. Voir ***Commencer avec un nouveau projet*** (page ***61***).

3.4.2.1. Commencer par la sélection de l'appareil

Créez un nouveau projet pour l'extraction de données basé sur un appareil connu.

1) Dans la fenêtre Ouvrir (avancé), cliquez sur **Sélectionner l'appareil**.



2) Dans la liste **Sélectionner l'appareil**, sélectionnez l'appareil souhaité.
3) Utilisez la liste de fabricants sur la gauche pour filtrer les appareils affichés par fabricant, et le champ **Filtre rapide** pour filtrer les appareils affichés en fonction d'une chaîne.

4) Cliquez sur **Suivant**.

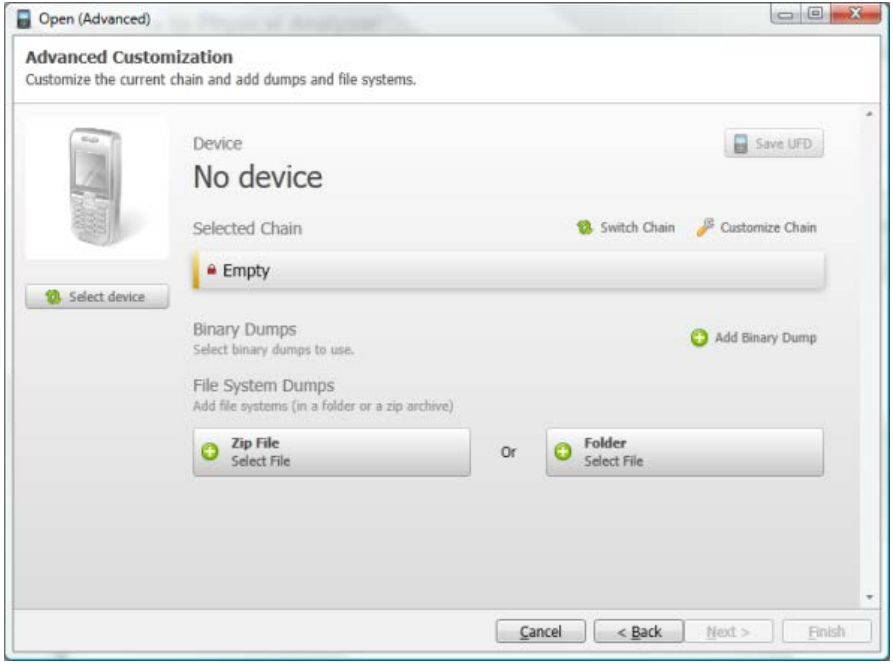
   Le panneau Personnalisation avancée affiche le nom et la chaîne de décodage par défaut de l'appareil sélectionné.

   - Pour sélectionner un appareil différent, consultez la section ***Spécifier un appareil différent*** (page ***47***).
   - Pour sélectionner une chaîne d'analyse différente, consultez la section ***Spécifier une chaîne différente*** (page ***50***).
   - Pour personnaliser la chaîne d'analyse, consultez la section ***Modifier la chaîne actuelle*** (page ***51***).
   - Pour ajouter des extractions binaires, consultez la section ***Ajouter un vidage binaire*** (page ***55***).
   - Pour ajouter une extraction de système de fichiers, consultez la section ***Ajouter un vidage de système de fichiers*** (page ***56***).

5) Cliquez sur **Terminer**.

3.4.2.2. Commencer avec un nouveau projet

1) Dans la fenêtre Ouvrir (avancé), cliquez sur **Nouveau projet**.



2) Pour sélectionner un appareil, consultez la section ***Spécifier un appareil différent*** (page ***47***).
3) Pour sélectionner une chaîne d'analyse, consultez la section ***Sélectionner une chaîne différente*** (page ***50***).

4) Pour personnaliser la chaîne d'analyse, consultez la section ***Modifier la chaîne actuelle*** (page ***51***).
5) Pour ajouter des extractions binaires, consultez la section ***Ajouter un vidage binaire*** (page ***55***).
6) Pour ajouter une extraction de système de fichiers, consultez la section ***Ajouter un vidage de système de fichiers*** (page ***56***).
7) Cliquez sur **Terminer**.

3.4.2.3. Extractions JTAG

JTAG (Joint Test Action Group) est une méthode d'extraction de données avancée qui nécessite un expert pour la connexion aux ports d'accès de test de l'appareil pour obtenir une image physique complète. Cela permet à l'expert de déverrouiller les données brutes stockées sur la puce de mémoire et d'y accéder.

JTAG est une méthode non destructrice et permet d'accéder aux données sur des appareils altérés ou endommagés, sur lesquels les ports de données ne sont pas disponibles (ou déconnectés), ou lorsqu'il est impossible de déverrouiller l'appareil à l'aide des autres outils d'investigation.

UFED Physical Analyzer automatise le processus de décodage JTAG et vous permet de gagner du temps, car il devient inutile de décoder manuellement les importants volumes de données brutes obtenus grâce aux extractions avec la méthode JTAG. Le tableau suivant répertorie une partie des appareils pris en charge :

Fournisseur	Modèle
Casio	C711 GzOne Boulder C751 GzOne Ravine
HTC	A7272 Desire Z Google Nexus One
Huawei	M860 Ascend Ascend Y300 (Android)
Kyocera CDMA	S2100 S2300 Torino (CommonCents)
LG CDMA	LX-290 VS-740 Ally
Nokia	Lumia 520 Lumia 920
Pantech	Razzle TXT8030VW (Verizon Wireless) Renue P6030
Samsung GSM	SGH-i337 Galaxy S4 SGH-i437 Galaxy Express
Sanyo CDMA	SCP-2700 Juno
T-Mobile	Touch Pro 2

ZTE GSM	Z221

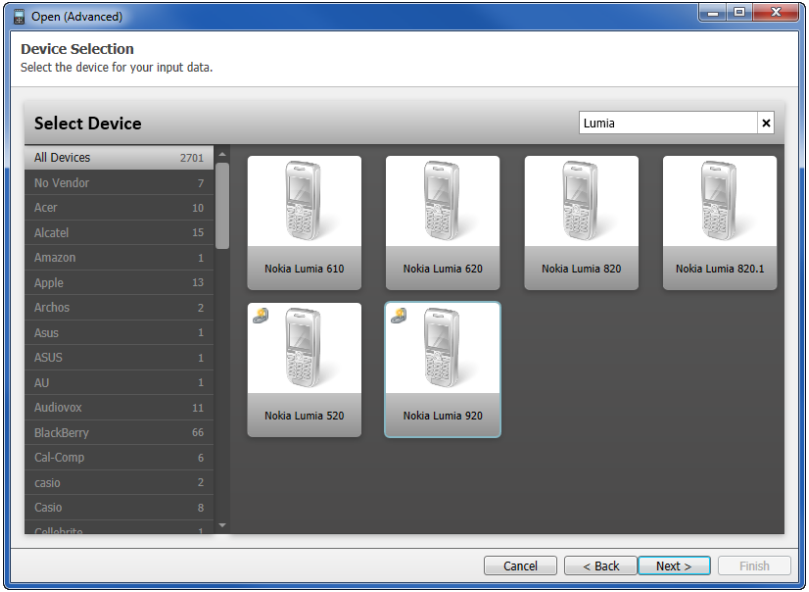
Pour consulter la liste à jour des appareils qui prennent en charge les extractions JTAG, reportez-vous à l'application UFED Phone Detective Mobile ou rendez-vous sur le site http://www.cellebrite.com/mobile-forensics/support/ufed-supported-devices.

Une fois que vous disposez de la mémoire physique acquise par le biais de cette méthode, vous pouvez la charger dans UFED Physical Analyzer pour la décoder. Lorsque vous chargez la chaîne JTAG UFED concernée, vous recevez toutes les données, comme lors d'une extraction classique.

La principale différence entre une extraction JTAG et une extraction UFED réside dans l'emplacement des « spares » à l'intérieur de l'extraction. « Spares » est le terme technique qui désigne les métadonnées de blocs à l'intérieur de l'extraction. Elles peuvent se trouver à différents endroits dans l'extraction. Dans les extractions classiques, elles se trouvent à la fin de chaque bloc. Dans les extractions JTAG, elles se trouvent à la fin de l'extraction.

Pour décoder l'extraction de données à l'aide de JTAG :

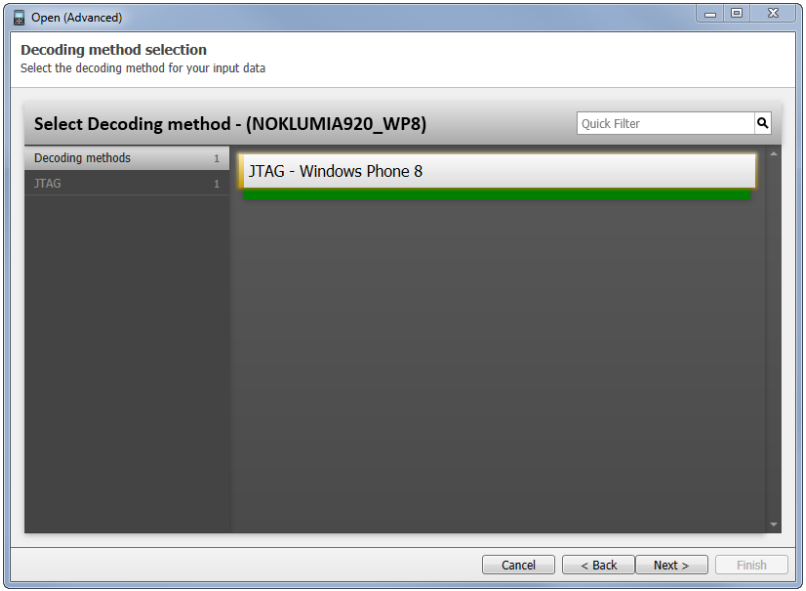
1) Dans la fenêtre Ouvrir (avancé), cliquez sur **Sélectionner l'appareil**.
2) Pour filtrer les appareils affichés, saisissez le nom de fabricant ou le modèle de l'appareil dans le champ **Filtre rapide**, ou cliquez sur le fabricant dans la liste de fabricants sur le panneau de gauche.



REMARQUE : Si la méthode JTAG n'est pas prise en charge pour l'appareil souhaité, vous pouvez saisir « jtag » dans le champ Filtre rapide pour sélectionner un appareil JTAG générique.

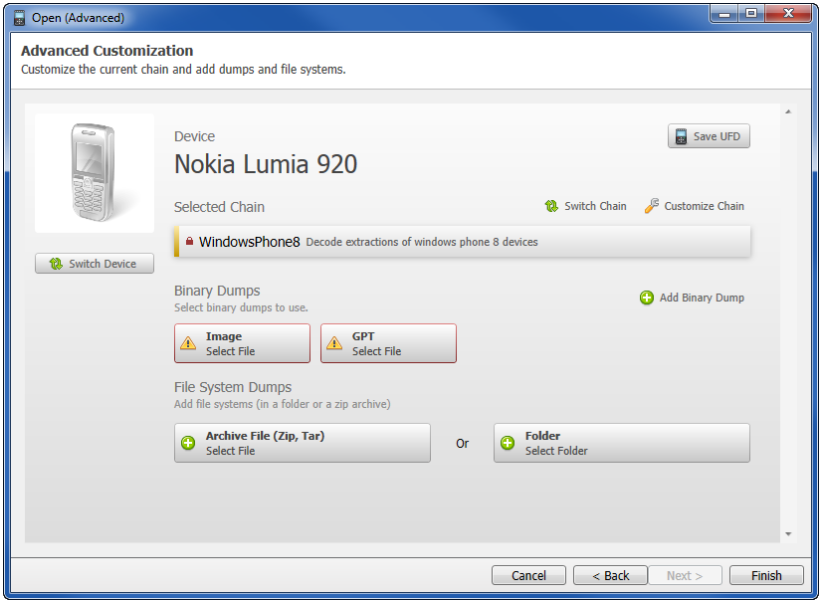
3) Sélectionnez l'appareil souhaité et cliquez sur **Suivant**.

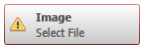
La fenêtre suivante s'affiche :



4) Sélectionnez la méthode de décodage et cliquez sur **Suivant**. Les méthodes disponibles varient en fonction de l'appareil.

La fenêtre suivante s'affiche :



5) Pour ajouter un fichier de vidage binaire, cliquez sur 

ou **Ajouter un vidage binaire** dans la zone **Vidages binaires**, et sélectionnez le fichier d'extraction binaire que vous souhaitez

ajouter. Chaque vidage binaire ajouté s'affiche comme composant distinct dans la section **Vidages binaires** de la boîte de dialogue.

6) Cliquez sur **Terminer**.

3.4.3. Enregistrement d'un fichier .ufd

À tout moment au cours de la configuration des paramètres Ouvrir (avancé), vous pouvez cliquer sur **Enregistrer UFD** dans l'angle supérieur droit de la boîte de dialogue pour enregistrer un fichier *.ufd qui contient les extractions binaires sélectionnées et les informations concernant l'appareil, pour une utilisation ultérieure.

La prochaine fois que vous aurez besoin de décoder ce fichier, vous pourrez utiliser le fichier UFD enregistré pour l'ouvrir avec **Ouvrir** ou **Ouvrir (avancé)**.

3.5. Enregistrer une session de projet

Enregistrez la session de projet pour sauvegarder votre travail. Vous pourrez ainsi fermer UFED Physical Analyzer et reprendre votre session plus tard.

Le fichier de session (.pas) enregistré inclut :

- La sélection de l'utilisateur dans les tableaux Données analysées et Fichiers de données,
- Des signets hexadécimaux,
- Des signets d'entités,
- Les résultats de la liste de surveillance,
- Les onglets ouverts,
- Les rapports générés.

Il est également possible de créer une session de projet pour les extractions effectuées par des outils tiers.

REMARQUE : Les sessions de projet enregistrées ne contiennent pas de paramètres définis. Pour en savoir plus sur comment enregistrer vos paramètres, consultez la section ***Enregistrer les paramètres*** (page ***371***).

Pour enregistrer une session de projet :

1) Dans le menu **Fichier**, sélectionnez **Enregistrer une session de projet**.

   La boîte de dialogue « Enregistrer sous » s'affiche.

2) Accédez à l'emplacement dans lequel vous souhaitez enregistrer le fichier de la session de projet.
3) Pour changer le nom du fichier, modifiez le nom attribué automatiquement dans la zone de texte **Nom du fichier**.

   REMARQUE : Pour remplacer une session précédente, choisissez le même nom de fichier.

4) Cliquez sur **Enregistrer**.

3.6. Charger une session de projet

1) Dans l'onglet **Accueil**, ouvrez le projet avec lequel vous souhaitez travailler.
2) Dans le menu **Fichier**, sélectionnez **Charger une session de projet**.
3) Dans la boîte de dialogue Ouvrir, accédez au fichier de session de projet que vous souhaitez ouvrir.
4) Cliquez sur **Ouvrir**.

   La session s'ouvre.

3.7. Fermer un projet

- Utilisez une des méthodes suivantes :
    - Dans le menu **Fichier**, sélectionnez **Fermer**.
    - Cliquez avec le bouton droit de la souris sur le nom du projet et sélectionnez **Fermer**.

3.8. Fermer UFED Physical Analyzer

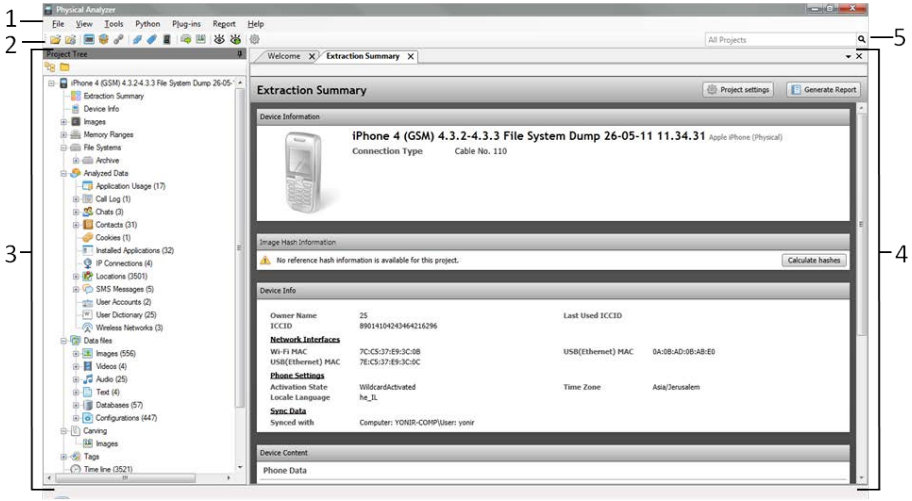
- Dans le menu **Fichier**, sélectionnez **Quitter**.

3.9. Raccourcis clavier

Ctr+O	Ouvrir un fichier
Ctr+W	Fermer un projet
Ctrl+P	Ouvrir les paramètres du projet
Ctrl+Maj+O	Ouvrir (avancé)
Ctrl+I	Ouvrir l'assistant iOS
Ctrl+T	Ouvrir les paramètres
Espace	Cocher ou décocher les cases
Ctrl+R	Ouvrir l'assistant de création de rapports
Ctrl+Tab	Passer d'un onglet ouvert à un autre
Ctrl+Début	Placer le curseur au début d'un tableau
Ctrl+Fin	Placer le curseur à la fin d'un tableau
Ctrl+B	Ajouter un signet d'entité
Ctrl+J	Extraire GPS ou appareil de stockage de masse
Ctrl+U	Ouvrir l'application de téléchargement UFED pour se connecter à UFED
Ctrl+D	Sélectionner un dossier pour le vidage du système de fichiers

Chapitre 4 : **S'orienter dans l'espace de travail**

L'espace de travail se compose de deux zones principales : l'arborescence de projet et la zone d'affichage des données permettant de simplifier votre travail.



L'espace de travail comprend les composants suivants :

1) Barre de menu de l'application
2) Barre d'outils de l'application
3) Arborescence de projet
4) Zone d'affichage de données
5) Recherche dans tous les projets

4.1. Arborescence de projet

La zone **Arborescence de projet** affiche la structure des informations extraites suivante pour chaque projet ouvert, pour analyse :

Élément de l'arborescence	Description
Résumé d'extraction	• Double-cliquez sur **Résumé d'extraction** pour ouvrir un résumé du projet dans la zone d'affichage des données. Pour plus d'informations, consultez la section ***Onglet Résumé d'extraction*** (page ***94***).

Élément de l'arborescence	Description
Infos appareil	• Double-cliquez sur **Infos appareil** pour ouvrir un onglet dans la zone d'affichage des données. L'onglet **Infos appareil** fournit une liste des informations existantes, ainsi que des identifiants importants pour l'appareil, notamment les codes de carte SIM et de verrouillage de l'utilisateur, le cas échéant. Le nombre de catégories et la quantité d'informations affichées varie en fonction du modèle et du fabricant de l'appareil.
Images	• Double-cliquez sur une image pour l'afficher dans un onglet Vue hexadécimale dans la zone d'affichage des données. L'élément d'arborescence **Images** répertorie tous les fichiers d'extraction générés depuis les modules de mémoire de l'appareil.

Élément de l'arborescence	Description

Plages mémoire	L'élément d'arborescence **Plages mémoire** répertorie les plages de mémoire analysées pour chaque module de mémoire extrait de l'appareil (répertoriés sous **Images**).
	• Sélectionnez une plage mémoire pour :
	  • Mettre en évidence la portion de la plage mémoire dans les données affichées.
	  • L'ajouter à la liste des mises en évidence de l'image binaire affichée à laquelle elle appartient (située en bas de l'onglet Vue hexadécimale).
	• Double-cliquez sur une plage mémoire pour afficher son contenu dans un nouvel onglet Vue hexadécimale.

Élément de l'arborescence	Description
Systèmes de fichiers	L'élément d'arborescence **Systèmes de fichiers** répertorie tous les systèmes de fichiers trouvés ou reconstruits à partir du fichier binaire analysé. Chaque système de fichiers porte la mention (disque dur). Les fichiers supprimés sont indiqués par une croix rouge ( ). • Double-cliquez sur un système de fichiers pour afficher son contenu dans un nouvel onglet Vue hexadécimale.

Élément de l'arborescence	Description
Données analysées	L'élément d'arborescence **Données analysées** affiche les groupes de données analysées correspondant à des fonctionnalités spécifiques de l'appareil, telles que les contacts, les SMS, les journaux d'appel, etc. Les informations disponibles et ce qui s'affiche varient en fonction des fonctionnalités de l'appareil et de la version de l'application. Par exemple, les SMS sont triés en fonction des dossiers utilisés par la fonctionnalité de messagerie de l'appareil (Brouillons, Reçus, Envoyés, etc.). Les e-mails sont triés en fonction du compte de messagerie avec lequel ils ont été envoyés ou reçus. Un dossier « Compte ou messages non classés » répertorie les dossiers ou messages qui ne peuvent être classés dans aucun des comptes ou dossiers de compte trouvés (Brouillons, Reçus, Envoyés, etc.).

Élément de l'arborescence	Description
	Les types d'informations suivants peuvent s'afficher dans les **Données analysées** : • Informations personnelles : calendrier, contacts, notes, journal d'appels, dictionnaires utilisateur, comptes utilisateur ; • Éléments de messagerie : SMS, MMS, e-mails, messages instantanés, chat ;

Élément de l'arborescence	Description
	• Éléments de navigateur Web : signets, historique, cookies ; • Informations GPS : localisations (y compris de fichiers vidéo, métadonnées et bases de données SQLite), trajets, correctifs. Pour en savoir plus sur les géolocalisations, consultez la section ***À propos des données de localisation*** (page ***149***). • Informations de l'appareil : appairages Bluetooth, réseaux sans fil, données SIM, utilisation de l'application, Wi-Fi, localisations cellulaires. Le nombre entre parenthèses indique le nombre d'éléments que contient chaque catégorie. En sélectionnant une catégorie de données analysées, vous l'ajoutez automatiquement à la liste des mises en évidence de l'image binaire et/ou de la plage mémoire affichée à laquelle elle appartient (située en bas de l'onglet Vue hexadécimale). Cela met également en évidence ses portions de plage de données dans les données affichées.

Élément de l'arborescence	Description
Fichiers de données	L'élément d'arborescence **Fichiers de données** trie les données extraites en formats de fichier communs ou connus, utilisés par les appareils et ordinateurs : images, vidéos, fichiers audio, fichiers texte ou documents. Dans l'arborescence de projet, les informations affichées sont triées selon les catégories suivantes : • **Images** – Fichiers reconnus comme des fichiers image • **Vidéos** – Fichiers reconnus comme des fichiers vidéo • **Audio** – Fichiers reconnus comme des fichiers audio • **Texte** – Fichiers reconnus comme des fichiers texte • **Bases de données** – Structures de données reconnues comme des bases de données • **Configurations** – Fichiers de configuration de l'appareil (tels que les fichiers .plist iOS)

Élément de l'arborescence	Description
	• **Applications** – Fichiers reconnus comme des fichiers d'application (fichiers .apk, .jar, .dex, .so, .exe, etc.) • **Documents** – Fichiers reconnus comme des fichiers documents (fichiers .doc, .docx, .pdf, .xlsx, .ppt, etc.) Les éléments supprimés sont indiqués par une croix rouge ( ). Vous pouvez créer des groupes de fichiers de données supplémentaires. Pour plus d'informations, consultez la section ***Gérer les paramètres des fichiers de données*** (page ***349***).
Reconstitution	L'élément d'arborescence **Reconstitution** vous permet d'effectuer une recherche dans l'extraction physique pour trouver des images partiellement supprimées ou corrompues. • Double-cliquez sur **Reconstitution** pour lancer la recherche. Pour plus d'informations, consultez la section ***Reconstituer des images*** (page ***239***).

Élément de l'arborescence	Description
Balises	Certains types de fichiers sont identifiés et balisés dans les données extraites. Il existe huit balises par défaut : **Applications**, **Audio, Configurations, Bases de données, Documents, Images**, **Texte** et **Vidéos**. Vous pouvez utiliser les plug-ins ou le shell Python pour rechercher des segments de données supplémentaires et les baliser à l'aide des balises existantes, ou d'une balise personnalisée. Les éléments supprimés sont indiqués par une croix rouge ( ).
Chronologie	• Double-cliquez sur **Chronologie** pour ouvrir les événements de l'appareil organisés par ordre chronologique dans la zone d'affichage des données. L'onglet **Chronologie** affiche les événements horodatés de l'appareil : appels, SMS, MMS, etc. dans l'ordre chronologique.

Élément de l'arborescence	Description
Listes de surveillance	Les listes de surveillance sont des listes de mots clés que vous créez et utilisez pour rechercher et identifier des événements et éléments spécifiques dans les données extraites. • Développez les **Listes de surveillance** pour afficher une liste des listes de surveillances exécutées au cours de la session actuelle. • Double-cliquez sur **Listes de surveillance** pour afficher les entités mises en évidence en fonction des listes de surveillance. Pour plus d'informations, consultez la section ***Travailler avec les listes de surveillance*** (page 132***132***).
Signets	Les signets que vous créez pour définir et enregistrer des emplacements spécifiques dans les données hexadécimales sont gérés dans l'élément d'arborescence **Signets**. • Double-cliquez sur **Signets** pour ouvrir une liste des signets dans un onglet dans la zone d'affichage des données.

Élément de l'arborescence	Description
Des signets d'entités	Les signets d'entités que vous créez sont gérés dans l'élément **Signets d'entités** de l'arborescence du projet. Le nombre de signets d'entités du projet apparaît entre parenthèses à côté du nom de la section. • Double-cliquez sur **Signets d'entités** pour ouvrir une liste des signets d'entités dans un onglet dans la zone d'affichage des données. • Double-cliquez sur un signet d'entité pour aller à l'élément marqué dans l'onglet d'affichage correspondant. Par exemple, double-cliquez sur un signet d'entité correspondant à un SMS pour ouvrir la liste de SMS dans un onglet d'affichage des Données analysées, avec l'élément marqué mis en surbrillance. Pour plus d'informations, consultez la section ***Informations sur les signets (signets d'entités)*** (page ***145***).

Élément de l'arborescence	Description
Rapports	Pour ouvrir un rapport qui a déjà été créé pour le projet : • Double-cliquez sur le rapport dans l'élément d'arborescence **Rapports**. Le rapport s'ouvre dans l'application associée au format du rapport. • Si aucun rapport n'a été créé pour le projet, double-cliquez sur l'élément d'arborescence **Rapports** pour ouvrir la boîte de dialogue Générer un rapport. Pour en savoir plus sur la création d'un rapport, consultez la section Générer un rapport.
Scanner anti-malware	Exécutez le scanner anti-malware pour identifier les malware sur l'appareil. Pour plus d'informations, consultez la section ***Rechercher les malware*** (page ***177***).

Élément de l'arborescence	Description
Analyse de projet	L'élément d'arborescence **Analyse de projet** fournir une présentation de l'analyse comparative. Vous pouvez ouvrir un onglet Analyse d'activité pour afficher une présentation de la totalité de l'activité de l'appareil, ainsi que des onglets correspondants aux activités du téléphone, des e-mails, de WhatsApp, de Skype, de Gmail et de BlackBerry Messenger. Pour plus d'informations, consultez la section ***Définir les paramètres du projet*** (page ***372***).

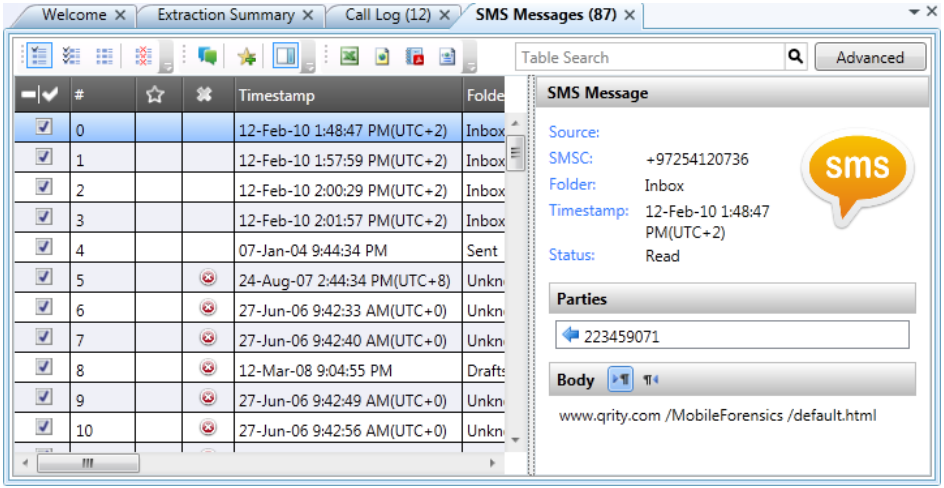
4.1.1. Travailler dans la zone Arborescence de projet

Ouvrez les éléments d'arborescence pour étudier et localiser des informations spécifiques :

- Cliquez pour développer ou pour réduire les éléments de l'arborescence.
- Double-cliquez sur un élément de l'arborescence pour ouvrir les informations détaillées dans la zone d'affichage des données.
- Cliquez sur en haut de l'arborescence du projet pour développer tous les éléments de celle-ci.
- Cliquez sur en haut de l'arborescence du projet pour réduire tous les éléments de celle-ci.

4.2. Zone d'affichage de données

Double-cliquez sur un élément pour l'afficher dans un onglet. Un nouvel onglet est ouvert pour chaque élément.



Il existe cinq types d'onglet :

- Onglet **Accueil**.
- Onglet **Résumé d'extraction**.
- Onglets de **données**, avec sous-onglets qui présentent une vue particulière, en fonction des données.
- Onglet **Chronologie**.
- Onglet **Image** (vue hexadécimale).

La zone d'affichage de données affiche également des fenêtres supplémentaires telles que la fenêtre Trace et les résultats de la liste de surveillance.

Pour fermer un onglet :

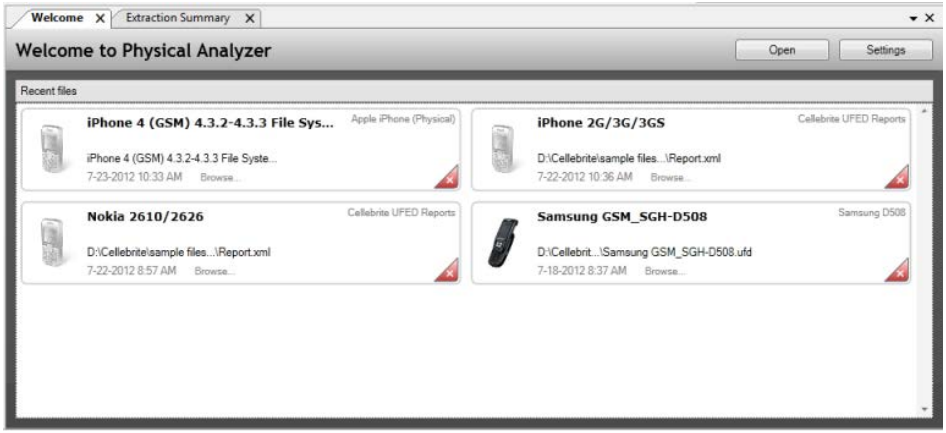
- Utilisez une des méthodes suivantes :
  - Cliquez sur ✕ sur l'en-tête de l'onglet.
  - Cliquez sur ✕ dans l'angle supérieur droit de la zone d'affichage des données.

Pour accéder à un onglet spécifique :

- Dans l'angle supérieur droit de la zone d'affichage de données, cliquez sur ▾, puis sélectionnez l'onglet souhaité dans la liste des onglets ouverts.

4.2.1. Onglet Accueil

L'onglet **Accueil** apparaît automatiquement dans la zone d'affichage des données au lancement de l'application. Il affiche une liste des fichiers ouverts récemment.



Chaque fichier dans la liste s'affiche sous la forme d'un groupe d'informations encadrées qui contient les éléments suivants :

- Image de l'appareil : image miniature de l'appareil tirée des ressources de l'application, lorsqu'elle est disponible. Lorsqu'aucune image n'est disponible, une image générique est utilisée.

- Nom du fichier : nom du fichier ouvert, sans l'extension.
- Chemin du fichier : chemin système vers le fichier.
- Modèle de l'appareil : fabricant et modèle de l'appareil identifié, ou « BINARY » si le fichier ouvert est une extension binaire.
- Nom du dossier : si un nom de dossier a été attribué au rapport, celui-ci s'affiche ici. Le nom peut être défini dans les paramètres du projet.
- Date et heure : date et heure de la dernière ouverture du fichier.
- Lien de navigation : lien direct vers le fichier dans le système.
- Supprimer élément récent : cliquez ici pour supprimer l'élément de l'onglet **Accueil**.

Vous pouvez procéder de la façon suivante :

- Cliquez sur un élément encadré pour ouvrir les fichiers à décoder.
- Cliquez sur **Parcourir** pour accéder directement au fichier associé dans le système de fichiers.
- Fermez l'onglet **Accueil**. Pour l'ouvrir à nouveau, allez dans **Vue** > **Afficher Accueil**.

4.2.2. Onglet Résumé d'extraction

L'onglet **Résumé d'extraction** s'affiche automatiquement lorsque vous ouvrez une nouvelle extraction pour analyse.

- Pour rouvrir l'onglet lorsqu'il est fermé, double-cliquez sur l'élément d'arborescence **Résumé d'extraction**.

L'onglet **Résumé d'extraction** peut afficher les informations suivantes :

- **Informations de l'extraction** : informations relatives à l'extraction de l'appareil. Telles que :

Date/heure début d'extraction *Date/heure fin d'extraction*	Début et fin de l'extraction
Identifiant d'unité	Numéro de série de l'appareil qui a effectué l'extraction (par ex. UFED Touch), ou un identifiant unique si l'extraction a été effectuée par une application PC (par ex. UFED 4PC)
Version d'unité	Version du logiciel UFED (par ex. 4.1.0.220)
Fabricant sélectionné	Fabricant de l'appareil (par ex. Apple)
Nom d'appareil sélectionné	Nom de l'appareil (par ex. iPhone 4)
Type de connexion	Câble utilisé pour l'extraction (par ex. Câble n° 100)
Type d'extraction	Type d'extraction effectué (par ex. système de fichiers)
ID d'extraction	ID unique pour chaque type d'extraction

- **Infos hachage d'image** : vérification des valeurs de hachage consignées pour les images analysées. Consultez la section ***Vérifier les valeurs de hachage*** (page ***244***).
- **Infos appareil** : résumé des informations spécifiques de l'appareil tirées du fichier d'extraction. Consultez l'élément *Infos appareil* dans ***Arborescence de projet*** (page ***76***).
- **Contenu de l'appareil** : contenu analysé, divisé en catégories :
    - **Données du téléphone** : type de données de l'appareil analysées trouvées lors de l'extraction (journal d'appels, contacts, SMS, etc.). Pour une liste complète des types de données de téléphone, consultez l'élément *Données analysées* dans ***Arborescence de projet*** (page ***76***).
    - **Fichiers de données** : type de fichiers de données standard trouvées lors de l'extraction (images, vidéos, fichiers audio et fichiers texte). Consultez la section ***Fichiers de données*** (page ***347***).

Pour afficher les informations correspondantes dans un nouvel onglet dans la zone d'affichage des données :

- Cliquez sur un élément de l'arborescence.

4.2.3. Onglets de données

Les onglets de données affichent les fichiers d'un type spécifique (journal d'appels, contacts, SMS, etc.).

Chaque type de fichier de données dispose de plusieurs modes d'affichage des données :

Fichiers d'application	**Vue hexadécimale** et **Infos fichier**
Fichiers images	**Vue hexadécimale**, **Vue image** et **Infos fichier**
Fichiers vidéo	**Vue hexadécimale**, **Info du fichier** et **Vue vidéo**
Fichiers audio	**Vue hexadécimale** et **Infos fichier**
Fichiers de texte	**Affichage texte, Vue hexadécimale** et **Infos fichier**
Fichiers documents	**Vue hexadécimale** et **Infos fichier**
Bases de données	**Vue base de données**, **Vue hexadécimale** et **Infos fichier**
Configurations	**Vue hexadécimale** et **Infos fichier**

Les onglets de données affichent les données dans plusieurs sous-onglets, selon le type de données :

- **Vue tableau** : liste de tous les fichiers d'un type spécifique (images, vidéos, fichiers audio, fichiers texte, etc.) trouvés au cours du processus d'analyse de données.
- **Vue dossier** : affiche la structure de dossiers des chemins des fichiers de données dans le système de fichiers reconstruit (pour les fichiers de données uniquement).
- **Vue hexadécimale** : affiche les données hexadécimales d'un élément binaire.
- **Vue image** : affiche l'image. Consultez la section ***Afficher les fichiers image*** (page ***116***).
- **Vue miniature** : affiche des miniatures des images (pour les images uniquement).
- **Infos fichier** : affiche les informations relatives au fichier.
- **Vue base de données** : affiche le contenu des fichiers de base de données.

4.2.3.1. Travailler dans les onglets de données

Sélectionner des éléments :

Sélectionnez les éléments dans la zone d'affichage des données pour les inclure dans un rapport que vous créez. Par défaut, tous les éléments sont sélectionnés.

- Pour sélectionner plusieurs éléments, maintenez la touche MAJ ou CTRL (pour une sélection consécutive ou non consécutive, respectivement).

- Lorsqu'un élément est sélectionné, appuyez sur la barre d'espace pour cocher ou décocher la case, afin d'indiquer si l'élément doit être inclus ou exclus du rapport.
- Pour sélectionner tous les éléments, cochez la case dans l'en-tête de la colonne (vue tableau et chronologie) ou cochez la case **Tout sélectionner** (vue miniature).

Trier les colonnes :

Vous pouvez trier chaque colonne par ordre alphabétique ou chronologique.

- Cliquez sur l'en-tête de la colonne pour modifier l'ordre de tri.

Réorganiser les colonnes :

Vous pouvez modifier l'ordre des colonnes à votre convenance. Votre préférence sera conservée pour la durée de la session.

- Faites glisser chaque colonne jusqu'à l'emplacement souhaité.

Afficher ou masquer les colonnes :

- Cliquez avec le bouton droit de la souris sur l'en-tête de la colonne et sélectionnez le nom de la colonne dans la liste.

Afficher des informations supplémentaires :

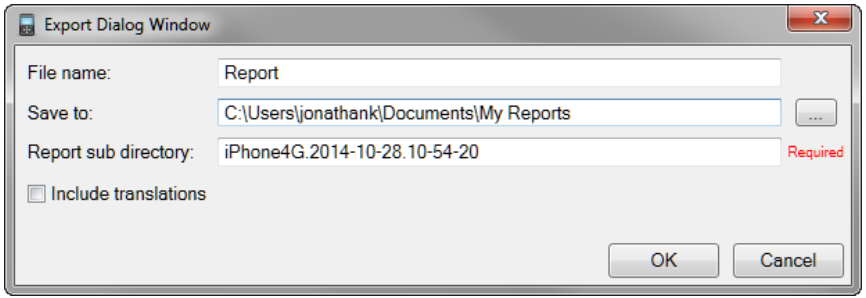
Pour les onglets de données qui contiennent des informations sous forme de texte, le panneau de droite est ouvert par défaut, et affiche les informations relatives à l'élément sélectionné.

- Pour ouvrir ou fermer le panneau de droite, cliquez sur .

Exporter des données :

1) Pour exporter des données vers un onglet spécifique, cliquez sur le format souhaité dans la barre d'outils : Excel , HTML , PDF , XML , KML (données de positionnement uniquement) ou EML (données d'e-mail uniquement).

   La fenêtre de dialogue Exporter s'affiche.



2) Utilisez une des méthodes suivantes :
   - Saisissez le chemin de l'emplacement où vous souhaitez sauvegarder le rapport.
   - Cliquez sur ... et sélectionnez l'emplacement souhaité.
3) Cochez la case **Inclure les traductions** pour inclure les données traduites.
4) Cliquez sur **OK**.

Le rapport est créé, et un message s'affiche, vous demandant si vous souhaitez l'ouvrir avec un logiciel tiers.

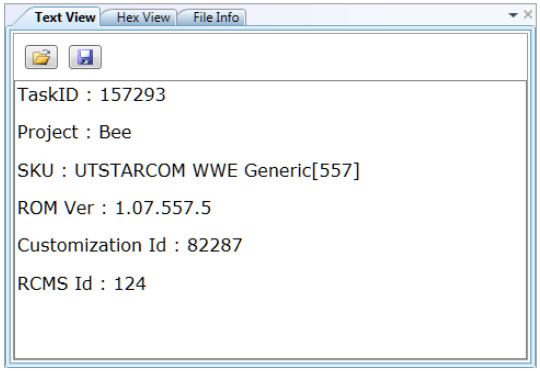
5) Cliquez sur **Oui** ou **Non**.

   Le fichier s'ouvre avec le logiciel tiers par défaut.

REMARQUE : Lorsque vous exportez un rapport au format EML, un fichier est créé pour chaque e-mail.

4.2.3.2. Vue texte

Pour les fichiers de données composés de texte, affichez les données dans un fichier texte.



4.2.3.3. Vue tableau pour les fichiers de données

Pour les fichiers de données, le tableau affiche les informations suivantes :

	Indique si l'élément doit être inclut (coché) ou exclu (décoché) dans le rapport généré.
N°	Numéro de ligne.
	Indique si l'élément est marqué par un signet.
	Indique si le fichier de données a été supprimé , ou si son état est inconnu (« ? » ou icône de document blanche).
Image	Une miniature de l'image ou une icône du type de fichier. (Fichiers de données image uniquement).
Nom	Nom du fichier.
Chemin	Chemin racine du fichier de données.

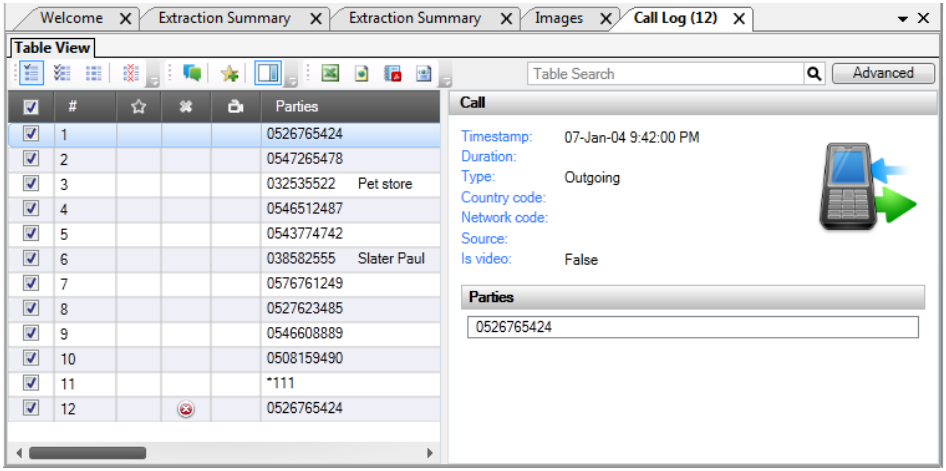
Taille	Taille du fichier.
Métadonnées	Métadonnées supplémentaires du fichier de données.
Date de création	Horodatage de création du fichier de données.
Modifié	Horodatage de modification du fichier de données.
Date d'accès	Horodatage du dernier accès au fichier de données.
Note de signet	Détails du signet.

En outre, des indicateurs s'affichent pour montrer les pièces jointes, indiquer les appels vidéo et même les directions.

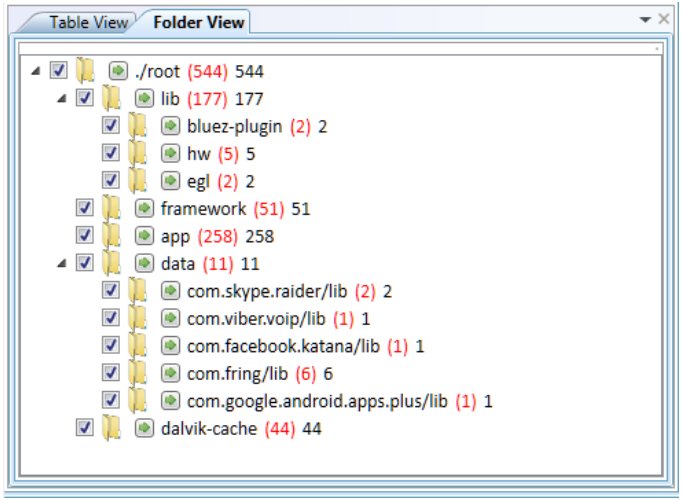
- Double-cliquez sur l'enregistrement d'un élément (ligne du tableau) pour ouvrir un onglet Vue hexadécimale montrant les données hexadécimales du fichier sélectionné.

4.2.3.4. Vue tableau pour les données analysées

Pour les données analysées, les onglets Vue tableau affichent une liste de tous les événements d'un type spécifique (journal d'appels, contacts, SMS, etc.) trouvés au cours du processus d'analyse de données.



4.2.3.5. Vue dossier



La vue dossier affiche l'organisation des éléments dans l'appareil.

- Cochez la case correspondant à un dossier pour sélectionner tous les éléments dans ce dossier (y compris les sous-dossiers). Les éléments sélectionnés seront inclus dans les rapports générés. Lorsque vous sélectionnez un élément, celui-ci est sélectionné dans tous les onglets dans la zone d'affichage des données.

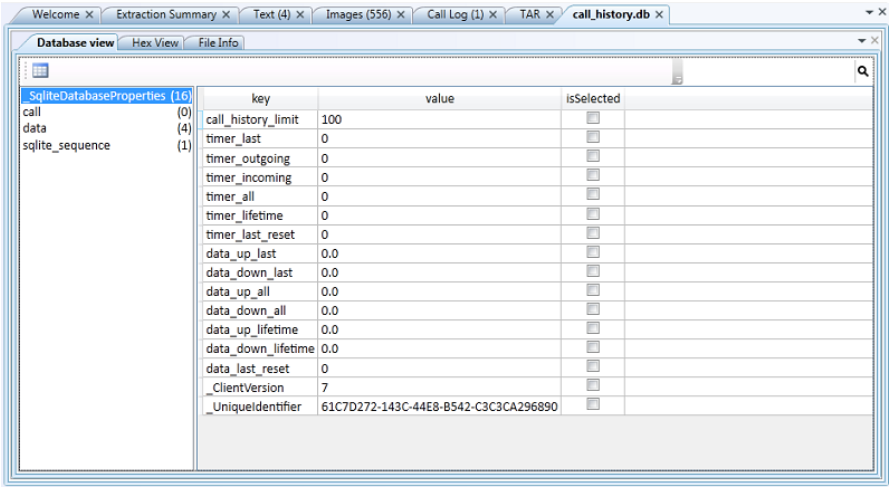
- Cliquez sur pour ouvrir le dossier dans un nouvel onglet dans la zone d'affichage des données.

Les informations suivantes relatives au dossier s'affichent :

- Le nom du dossier dans le système de fichiers extrait.
- Le nombre d'éléments sélectionnés dans ce dossier (en rouge et entre parenthèses).
- Le nombre total d'éléments dans ce dossier (en noir).

4.2.3.6. Vue base de données

- Pour ouvrir une vue base de données, ouvrez un fichier .db dans l'élément d'arborescence Systèmes de fichiers.



La vue base de données affiche le contenu des fichiers de base de données trouvés dans l'extraction.

La vue base de données se compose des sections suivantes :

1) Liste des tableaux de base de données.

Le nombre entre parenthèses à côté de chaque nom de tableau indique le nombre d'enregistrements dans le tableau de base de données.

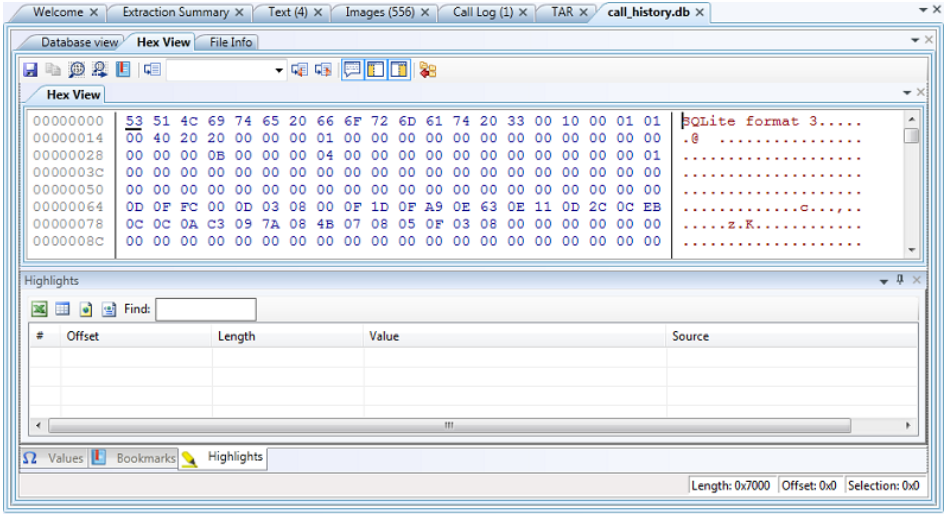
Sélectionnez un tableau dans la colonne de gauche pour afficher ses enregistrements dans la colonne de droite.

2) Les zones d'affichage des enregistrements contenant une liste des enregistrements de données dans le tableau de base de données sélectionné.
3) Un champ « Recherche » pour filtrer les enregistrements affichés.

- Cliquez sur pour exporter les enregistrements de base de données sélectionnés dans un fichier CSV.

4.2.3.7. Vue hexadécimale

Un onglet Vue hexadécimale apparaît pour chaque élément binaire ouvert à partir de l'arborescence de projet. Par exemple, lorsque vous ouvrez un disque mémoire Image, un onglet Vue hexadécimale s'ouvre seul. Lorsque vous ouvrez un élément binaire, par exemple un fichier image, l'onglet Vue hexadécimale peut être accompagné par d'autres onglets.



L'onglet Vue hexadécimale contient les sections suivantes :

Onglets hexadécimaux :

a) Colonne d'adresse : numéro de la colonne d'informations en valeur hexadécimale ou décimale, affichant l'adresse de départ de chaque ligne dans les sections de données de représentation hexadécimale et ASCII.

b) Colonne Vue de données hexadécimales : données hexadécimales de l'élément sélectionné.

c) Colonne Vue de représentation ASCII : représentation au format ASCII des données hexadécimales.

Une fenêtre d'informations s'affiche automatiquement lorsque vous placez la souris sur les informations affichées dans la vue hexadécimale. La fenêtre d'informations affiche des liens (pointeurs) vers les éléments de données analysés, tels que les fichiers et dossiers dans l'arborescence de projet, et les résultats de recherche associés aux données pointées.

Barre d'outils de la vue hexadécimale :

	Enregistrer	Cliquez ici pour enregistrer la totalité de l'extraction de mémoire dans un dossier local.
	Copier la sélection	Copie tous les contenus sélectionnés de l'onglet Vue hexadécimale vers le presse-papier.
	Rechercher	Affiche la boîte de dialogue Rechercher pour trouver toutes les occurrences des informations spécifiées dans le panneau d'affichage hexadécimal affiché.
	Rechercher suivant	Affiche la boîte de dialogue Rechercher avec les paramètres utilisés lors de la dernière recherche.
	Ajouter un signet	Ajoutez un signet au contenu sélectionné dans le panneau d'affichage hexadécimal.
	Aller à	Redirigez le décalage vers une adresse spécifique dans le contenu du panneau d'affichage hexadécimal.
	Activer la fenêtre d'infos	Active/Désactive l'affichage de la fenêtre d'infos flottante à l'emplacement du curseur.
	Afficher l'adresse	Active/Désactive l'affichage de la colonne d'adresse de gauche.
	Afficher en mode ASCII	Active/Désactive l'affichage de la colonne de représentation ASCII de droite.

Onglets d'informations sur l'analyse :

Les onglets d'informations sur l'analyse sont situés sous l'onglet Vue hexadécimale. Ils affichent les types d'informations suivants, en lien direct avec les données hexadécimales affichées :

- **Valeurs** : un grand nombre d'interprétations des valeurs, telles que 8, 16, 32 et 64 bits, divers encodages de chaîne, les formats de date et d'heure, etc., calculés au fur et à mesure pour les données actuelles contenues dans la vue hexadécimale. Consultez la section ***Travailler dans l'onglet Valeurs*** (page ***112***).
- **Signets** : une liste des signets ajoutés aux données hexadécimales affichées. Consultez la section ***Travailler avec les signets*** (page ***304***).
- **Mises en évidence** : une liste des segments de contenu mis en évidence dans les données hexadécimales affichées. Le nombre de résultats mis en évidence apparaît entre parenthèses à côté du nom de l'onglet. Consultez la section ***Travailler dans l'onglet Mises en évidence*** (page ***114***).
- **Rechercher** : affiche les résultats d'une recherche dans les données hexadécimales affichées. Un nouvel onglet Résultats de recherche est ouvert pour chaque recherche effectuée. Le nombre de résultats pour chaque recherche apparaît entre parenthèses à côté du nom de l'onglet.

Vous pouvez réorganiser les onglets d'informations sur l'analyse en fonction de vos préférences :

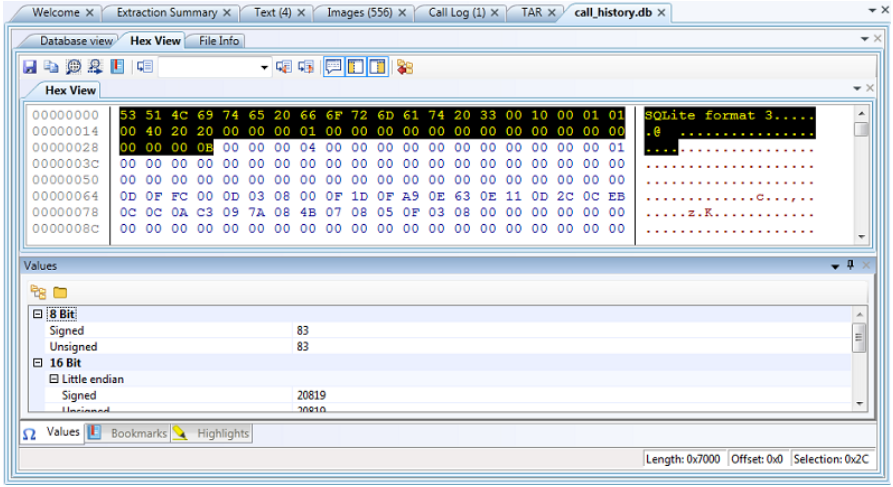
- Double-cliquez sur l'en-tête de la section pour afficher la totalité de celle-ci sous forme de fenêtre flottante. Double-cliquez sur l'en-tête de la fenêtre flottante pour l'ancrer à son emplacement par défaut (en bas de l'onglet Vue hexadécimale).

- Double-cliquez sur le nom d'un onglet pour l'afficher sous forme de fenêtre flottante. Double-cliquez sur l'en-tête de la fenêtre flottante pour l'ancrer à son emplacement d'origine.
- Faites glisser l'en-tête d'une fenêtre flottante jusqu'aux panneaux d'ancrage qui s'affichent pour l'ancrer à l'emplacement de votre choix dans la vue hexadécimale.

4.2.3.7.1. Travailler dans l'onglet Valeurs

Décodez les données brutes vers plusieurs types d'encodage en temps réel, et développez-les dans la liste Valeurs.

1) Pour accéder à l'onglet **Valeurs**, cliquez sur l'onglet **Valeurs** en bas d'un onglet **Vue hexadécimale**.



2) Sélectionnez un segment de données hexadécimales.
3) Pour afficher les données décodées, faites défiler les encodages jusqu'à celui que vous souhaitez, puis cliquez sur ⊞ pour agrandir l'affichage.

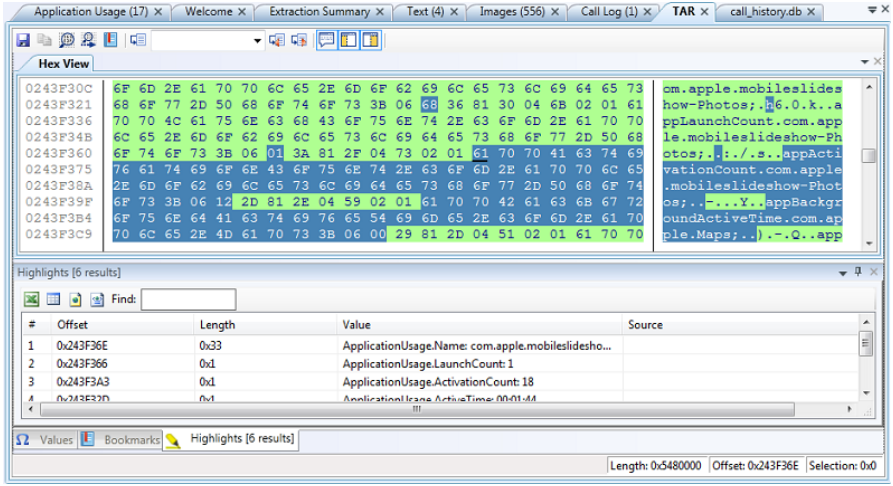
   Certaines options d'encodage, telles que le 16 bits, possèdent des types de sous-encodage.

4) Développez ou réduisez les types d'encodage en cliquant sur ou .

4.2.3.7.2. Travailler dans l'onglet Mises en évidence

L'onglet **Mises en évidence** contient une liste des segments de contenu mis en évidence dans les données hexadécimales affichées. Chaque segment représente l'emplacement des données analysées dans les données hexadécimales. L'onglet **Mises en évidence** vous permet de localiser des types de données analysées spécifiques dans les données hexadécimales. Le nombre de résultats mis en évidence apparaît entre parenthèses à côté du nom de l'onglet.

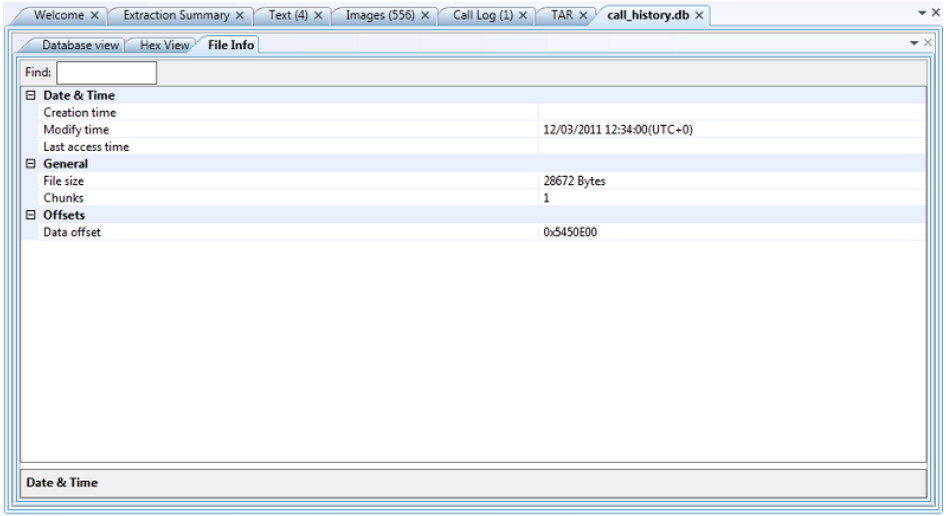
1) Pour accéder à l'onglet **Mises en évidence**, cliquez sur l'onglet **Mises en évidence** en bas d'un onglet **Vue hexadécimale**.



2) Dans l'arborescence de projet, cliquez sur un dossier **Données analysées** (par exemple **Contacts**).

   L'emplacement du dossier sélectionné est mis en évidence dans l'onglet **Vue hexadécimale**, et la liste des tranches de données qui composent le dossier se trouve dans l'onglet **Mises en évidence**.

4.2.3.8. Onglet Infos fichier



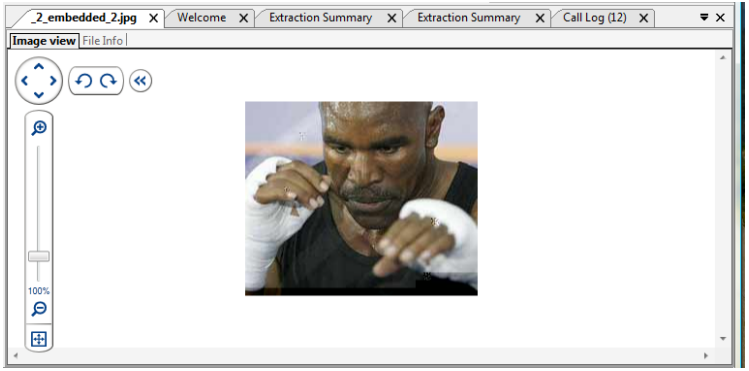
L'onglet Infos fichier affiche les informations suivantes relatives au fichier de données :

- **FAT** : table d'allocation de fichier des attributs étendus.
- **Date et heure** : horodatages de la date de création, de la date de modification et du dernier accès au fichier de données.
- **Général** : taille du fichier en octets et nombre de tranches du système de fichiers qui composent le fichier de données.
- **Décalages** : décalages d'adresse du fichier de données dans les données hexadécimales.
- **EXIF** : informations EXIF intégrées enregistrées par la caméra (le cas échéant).
- **Métadonnées du fichier** : informations générales concernant l'image (heure de capture, résolution, taille et profondeur de la couleur).

4.2.3.9. Afficher les fichiers images

1) Double-cliquez sur une image dans un onglet d'affichage des données.

Un nouvel onglet contenant l'image s'ouvre. Cet onglet est divisé en deux sous-onglets : **Vue image** et **Infos fichier**.



2) Dans l'onglet **Vue image**, utilisez les commandes de l'image :

Parcourir l'image, lorsqu'elle est agrandie.

Faire pivoter l'image dans le sens des aiguilles d'une montre et dans le sens inverse.

Zoom avant et arrière. Vous pouvez également ajuster le zoom à l'aide de la barre de glissement.

Faire un zoom avant pour ajuster l'image à l'onglet.

Redéfinir un zoom de 100 %.

Masquer les commandes de l'image.

3) Cliquez sur l'onglet **Infos fichier** pour afficher les informations relatives au fichier. Par exemple, la section Métadonnées de fichier inclut des informations telles que l'Heure de capture, qui correspond à la date et l'heure auxquelles la photo a été prise.

4.2.3.10. Lire des fichiers vidéo

Pour lire des fichiers vidéo avec UFED Physical Analyzer :

1) Dans le tableau de données, double-cliquez sur le fichier média que vous souhaitez lire.

   Un nouvel onglet s'ouvre pour le fichier média.

2) Cliquez sur .

Pour lire la vidéo avec le programme par défaut :

- Cliquez avec le bouton droit de la souris sur le fichier média et sélectionnez **Ouvrir avec le programme par défaut**.

Chapitre 5 : **Localisation et analyse des informations**

Cette section décrit comment parcourir, rechercher, filtrer, marquer par un signet et gérer les informations dans votre projet.

5.1. Rechercher des informations dans un onglet de données

Dans les onglets **Vue tableau**, recherchez un élément particulier dans le tableau de données. La recherche est effectuée sur toutes les entrées de données du tableau.

- Dans la case **Rechercher dans le tableau**, saisissez la chaîne de votre choix.

  Le tableau est mis à jour pour afficher uniquement les éléments qui contiennent la chaîne que vous avez saisie.

5.2. Utiliser le filtre rapide

Utilisez les outils du filtre rapide pour filtrer les données dans les onglets **Vue tableau** de la façon suivante :

	Tout afficher	Affiche tous les éléments.
	Sélectionné uniquement	Affiche les éléments sélectionnés.
	Non sélectionné uniquement	Affiche les éléments non sélectionnés.
	Supprimé	Affiche les éléments supprimés.
	Tout afficher	Affiche toutes les images.
	Afficher les images de plus de 30 Ko	Affiche uniquement les petites images de plus de 30 Ko.
	Afficher les images de plus de 100 Ko	Affiche uniquement les images de taille moyenne de plus de 100 Ko.
	Afficher les images de plus de 500 Ko	Affiche les grandes images uniquement (plus de 500 Ko).
	Filtrer les images (par extension)	Cliquez ici pour activer le filtre par type de fichier.

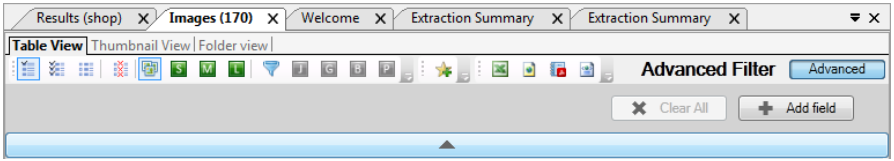
	Afficher les fichiers JPEG	Affiche les fichiers JPG ou JPEG.
	Afficher les fichiers GIF	Affiche les fichiers GIF.
	Afficher les fichiers BMP	Affiche les fichiers BMP.
	Afficher les fichiers PNG	Affiche les fichiers PNG.
	Filtre métadonnées	Filtrez les fichiers image et vidéo par métadonnées (Toutes, Sans métadonnées ou Contient des métadonnées) et par emplacement (Tous, Possède un emplacement ou Sans emplacement).
	Filtre heure de capture	Filtrez les fichiers image et vidéo en fonction de l'heure de capture. La plage maximum est affichée par défaut, et vous pouvez sélectionner une plage spécifique définie par une date et une heure.
	Filtre traduction	Filtrez le texte traduit pour afficher tout le texte, le texte traduit ou le texte non traduit.

REMARQUE : Les éléments de la barre d'outils varient selon le contexte, et s'affichent uniquement lorsque des données pertinentes sont affichées.

5.3. Utiliser le filtre avancé

Utilisez le filtre avancé pour filtrer la liste selon plusieurs paramètres.

1) Dans la barre d'outils du filtre, cliquez sur **Avancé**.



2) Cliquez sur **Ajouter un champ**, puis sélectionnez un champ dans la liste déroulante. La liste de champs se compose des colonnes dans l'onglet de données actuel.
3) Dans la case qui s'affiche pour le champ sélectionné, saisissez la chaîne ou l'horodatage de votre choix.

   L'onglet affiche uniquement les éléments correspondant au filtre.
4) Pour ajouter d'autres filtres, répétez les étapes 2 et 3.

   Lorsque vous ajoutez des filtres dans la recherche avancée, les résultats correspondent à tous les critères spécifiés.

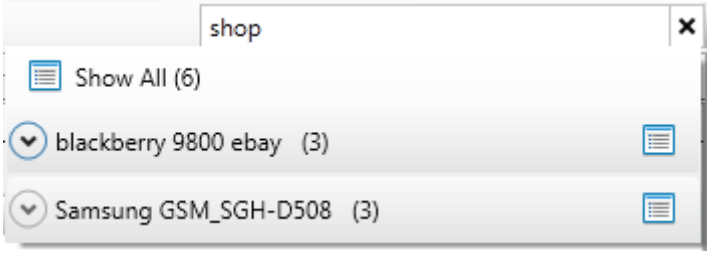
5) Pour effacer la chaîne saisie, cliquez sur .
6) Pour effacer toutes les chaînes saisies, cliquez sur **Tout effacer**.
7) Pour supprimer le filtre du champ, cliquez sur .
8) Pour fermer le filtre avancé, cliquez sur **Avancé**.

5.4. Rechercher des informations dans tous les projets ouverts

Utilisez la boîte de recherche **Tous les projets** dans la barre d'outils pour rechercher des informations dans tous les projets ouverts.

1) Saisissez la chaîne de votre choix dans la case **Tous les projets**.

   Une liste des résultats correspondants s'affiche sous le champ de recherche **Tous les projets**. Les résultats sont triés par projet ouvert. Dans chaque projet, les résultats sont triés par catégories, selon le type (SMS, messages, contacts, fichiers, etc.). Le nombre de résultats dans chaque catégorie type s'affiche également.



2) Cliquez sur pour réduire ou développer les projets.
3) Utilisez une des méthodes suivantes :
    - Cliquez sur à côté du nom d'un projet pour afficher les résultats de la recherche dans cette extraction dans un onglet, dans la zone d'affichage des données.
    - Sélectionnez **Tout afficher** en haut de la liste de résultats rapides pour afficher un onglet Résultats dans la zone d'affichage des données montrant tous les résultats de la recherche. La chaîne correspondante dans chaque élément apparaît en rouge.

    Comme dans la liste de résultats rapides, l'onglet Résultats répertorie les résultats par type.

5.5. Parcourir le système de fichiers

UFED Physical Analyzer permet de reconstruire et d'afficher le système de fichiers d'un appareil sous forme d'arborescence.

Pour parcourir le système de fichiers de l'appareil :

1) Dans l'élément d'arborescence **Systèmes de fichiers**, cliquez sur l'icône ◢ ou ▷ de chaque nœud pour développer l'élément correspondant.
2) Continuez à développer le système de fichiers pour explorer son contenu.

   Une des icônes suivantes est attribuée à chaque fichier du système de fichiers reconstruit :

   - - Fichier existant trouvé dans le système
   - - Fichier supprimé trouvé dans le système de fichiers
3) Pour ouvrir un fichier, double-cliquez dessus pour afficher ses informations dans la zone d'affichage des données.

   Le nombre d'onglets d'informations affiché pour un fichier varie en fonction du type de fichier. Par exemple, un fichier inconnu affiche uniquement les onglets **Vue hexadécimale** et **Infos fichier**, alors qu'une image au format JPEG peut également afficher les onglets **Vue image** et **Métadonnées**. La vue par défaut est la **Vue hexadécimale**.

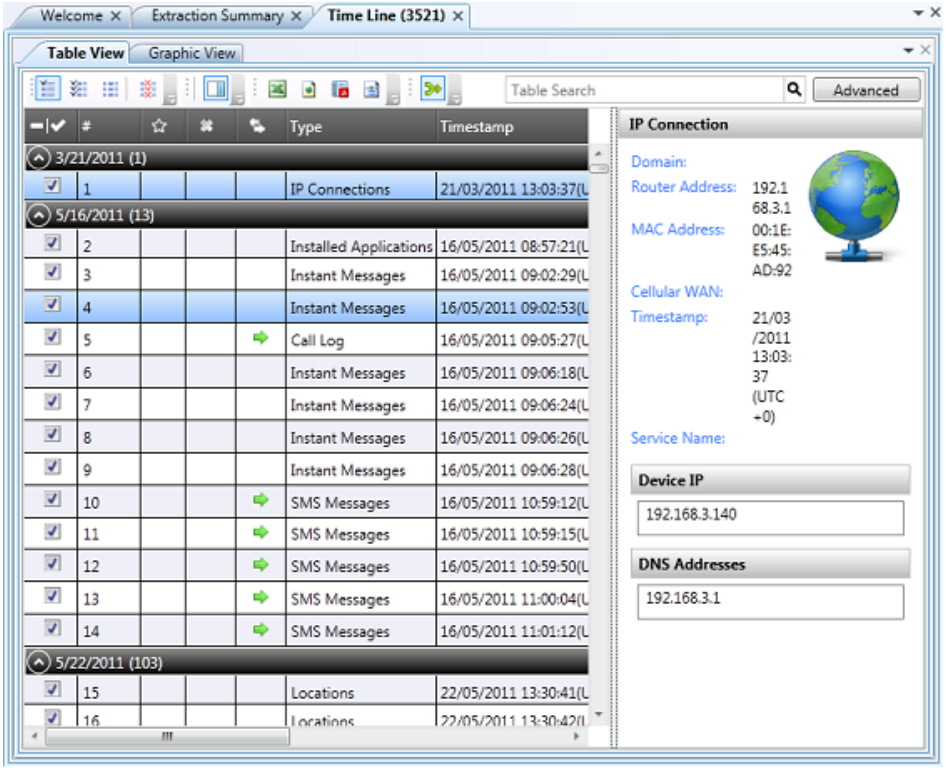
   Pour en savoir plus sur le travail avec la vue hexadécimale, consultez les sections ***Vue hexadécimale*** (page ***108***) et ***Travailler avec les données hexadécimales*** (page ***247***).
4) Lorsque l'extraction hexadécimale d'une image est affichée dans la zone d'affichage des données, cliquez sur un fichier sous l'élément d'arborescence **Systèmes de fichiers** pour mettre en évidence la portion de données de ce fichier dans les données hexadécimales dans la zone d'affichage des données.

5.6. Vue Chronologie

La vue Chronologie est un outil puissant qui vous permet d'analyser les données dans l'ordre chronologique, afin d'identifier l'ordre des événements et d'établir des liens entre eux.

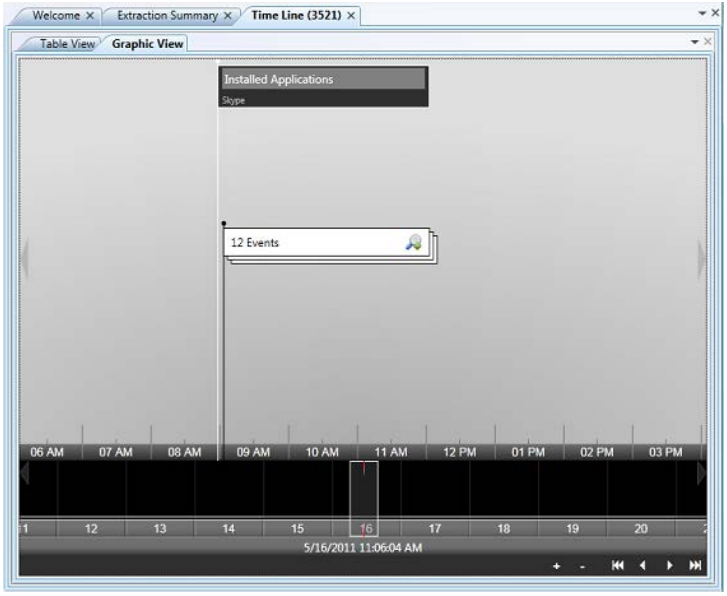
La vue Chronologie dispose de deux affichages : tableau et graphique.

Dans la vue tableau, les événements apparaissent dans un tableau, classés par date et heure.



- Cliquez sur pour regrouper ou séparer les événements en fonction de la date.

  Dans la vue graphique, les événements apparaissent dans un graphique. Cela vous permet d'identifier rapidement les pics d'activité potentiellement intéressants.



- Pour avancer ou reculer dans la chronologie, utilisez les boutons , , et .

Vous pouvez augmenter ou réduire le niveau de détail de la vue Chronologie :

- Pour augmenter la résolution temporelle, cliquez sur .
- Pour réduire la résolution temporelle, cliquez sur .

Les événements qui se produisent à peu d'intervalle sont marqués par groupes.

- Cliquez sur pour ouvrir un autre onglet Vue chronologie pour un groupe d'événements.

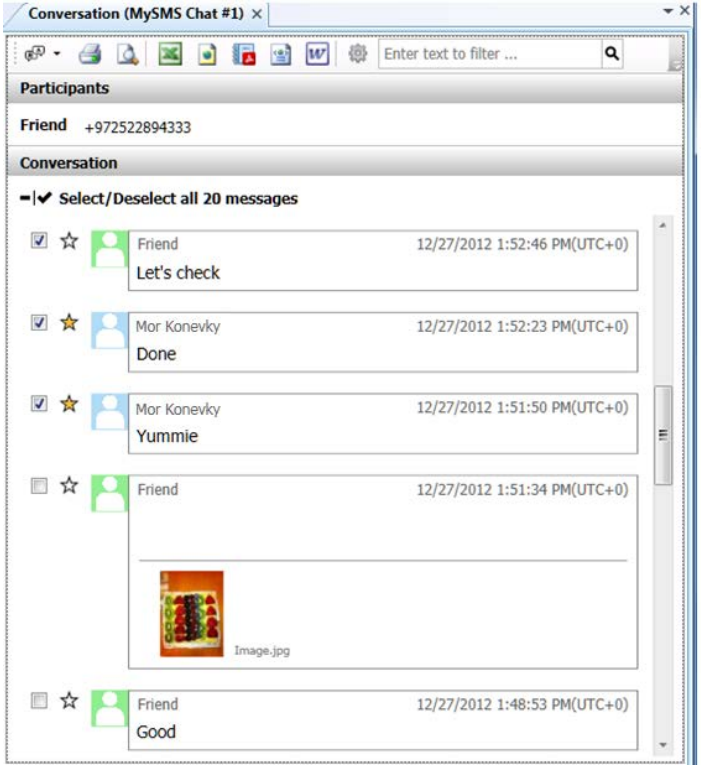
5.7. Accéder à la vue Conversation

Les données relatives aux communications (journaux d'appels, e-mails, SMS, MMS, etc.) peuvent être affichées dans une vue Conversation afin de suivre plus facilement et plus efficacement les communications entre deux parties ou plus. Vous pouvez rechercher des messages dans une conversation, sélectionner les messages à inclure dans un rapport (par défaut tous les messages de la conversation sont inclus), imprimer ou exporter la conversation.

Pour accéder à la vue Conversation et l'utiliser :

1) Dans un tableau de données relatives aux communications, sélectionnez l'un des enregistrements.
2) Cliquez sur .

   Un onglet Conversation s'ouvre, affichant les éléments correspondants sous forme de conversation entre l'expéditeur et le destinataire de l'élément sélectionné.


Conversation (MySMS Chat #1)
Enter text to filter ...
Participants
Friend +972522894333
Conversation
Select/Deselect all 20 messages
Friend 12/27/2012 1:52:46 PM(UTC+0)
Let's check
Mor Konevky 12/27/2012 1:52:23 PM(UTC+0)
Done
Mor Konevky 12/27/2012 1:51:50 PM(UTC+0)
Yummie
Friend 12/27/2012 1:51:34 PM(UTC+0)
Image.jpg
Friend 12/27/2012 1:48:53 PM(UTC+0)
Good

3) Pour traduire ou supprimer le texte traduit, cliquez sur et sélectionnez **Tout traduire** ou **Supprimer toutes les traductions**.
4) Pour imprimer la conversation, cliquez sur .
5) Pour afficher un aperçu avant impression, cliquez sur .
6) Pour exporter la conversation, cliquez sur le format souhaité dans la barre d'outils de l'onglet Conversation : Excel , HTML , PDF , XML ou Word .
7) Pour modifier l'ordre de la conversation, cliquez sur et sélectionnez **Message le plus ancien en premier** ou **Message le plus récent en premier**.
8) Pour filtrer les messages, saisissez le texte dans la zone de recherche.
9) Pour ajouter ou modifier des signets, cliquez sur .
10) Cochez une case pour inclure des messages spécifiques dans le rapport (ou sélectionnez Tous les messages ou Aucun message).

5.8. Travailler avec les listes de surveillance

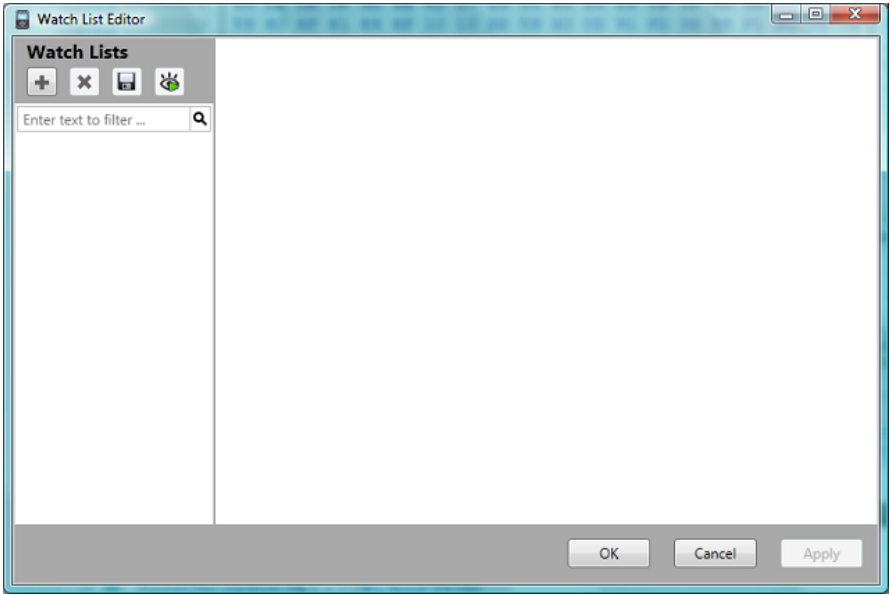
Exécutez une liste de surveillance composée de mots-clés sur vos données extraites afin d'identifier et de mettre en évidence les informations importantes et pertinentes.

La recherche par liste de surveillance peut être activée automatiquement ou exécutée manuellement sur les données décodées sélectionnées.

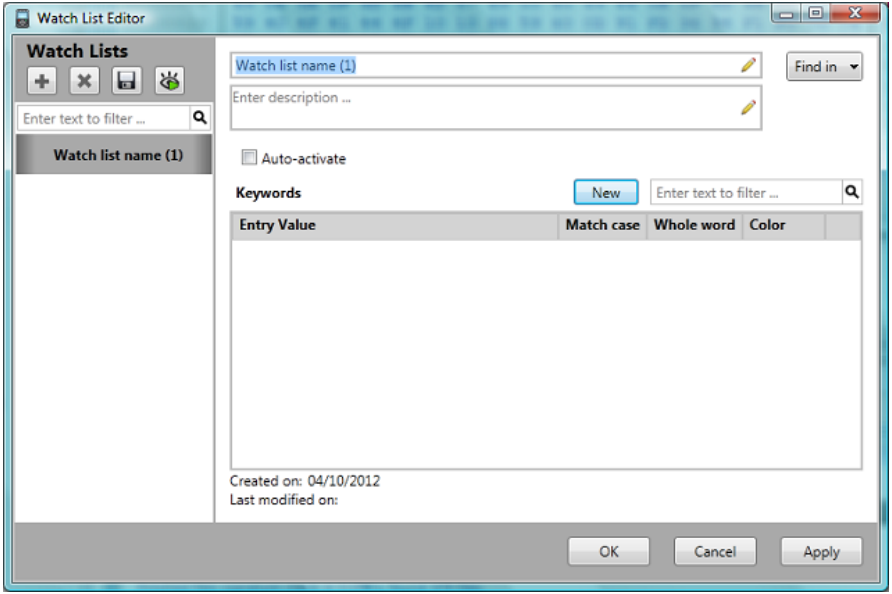
5.8.1. Créer une liste de surveillance

1) Utilisez une des méthodes suivantes :
    - Dans la barre d'outils, cliquez sur .
    - Dans le menu **Outils**, sélectionnez **Éditeur de liste de surveillance**.

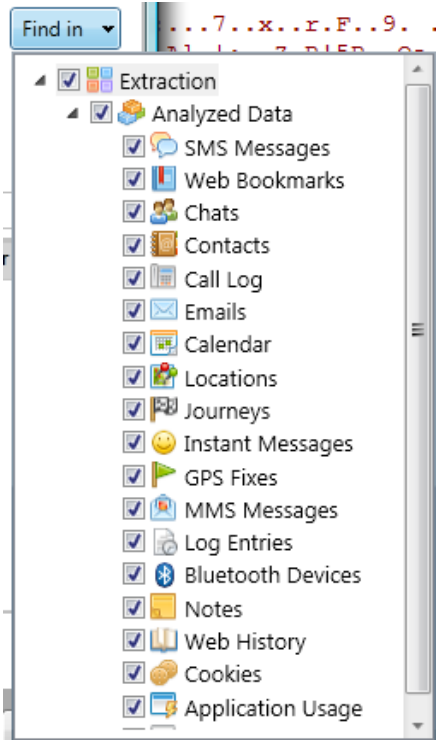
L'éditeur de liste de surveillance s'affiche.



2) Cliquez sur , et sélectionnez **Nouveau**.



3) Dans la case **Nom de la liste de surveillance**, saisissez le nom de la liste.
4) Pour que la liste de surveillance recherche les mots-clés uniquement dans les types de données dans le projet, cliquez sur **Rechercher dans**, puis sélectionnez les types de données souhaités.



Lorsque vous exécutez la liste de surveillance, seuls les types de données sélectionnés sont consultés pour y rechercher des correspondances.

5) Dans la case **Saisir une description**, saisissez une description générale de la liste de surveillance (facultatif).
6) Pour que la liste de surveillance soit exécutée automatiquement lorsque vous ouvrez un projet, cliquez sur **Activation auto**.
7) Cliquez sur **Nouveau** pour ajouter un mot-clé.

   Une ligne avec le nouveau mot-clé apparaît dans la liste des mots-clés.
8) Pour chaque mot-clé, définissez les options suivantes, à votre convenance :
   - **Valeur d'entrée** : Saisissez le mot clé.
   - **Respecter la casse** : Sélectionnez cette option pour respecter la casse du mot-clé.
   - **Mot entier** : Sélectionnez cette option pour rechercher le mot entier.
   - **Couleur** : Cliquez sur ▾ et sélectionnez la couleur d'affichage des mots-clés trouvés.
9) Utilisez une des méthodes suivantes :
   - Cliquez sur **Appliquer** pour enregistrer la liste de surveillance et garder l'éditeur de liste de surveillance ouvert.
   - Cliquez sur **OK** pour enregistrer la liste de surveillance et fermer l'éditeur de liste de surveillance.
   - Cliquez sur **Annuler** pour fermer l'éditeur de liste de surveillance sans enregistrer vos modifications.

5.8.2. Modifier une liste de surveillance

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez modifier.
2) Modifiez les paramètres et les mots-clés de la liste personnalisée, à votre convenance.
3) Pour filtrer la liste de mots-clés afin de localiser un mot-clé spécifique, saisissez celui-ci dans la case **Saisir le texte à filtrer**.
4) Pour modifier un mot-clé, cliquez sur celui-ci dans la liste, puis modifiez-le.
5) Pour supprimer un mot-clé, cliquez sur .
6) Lorsque vous avez terminé, procédez d'une des façons suivantes :
    - Cliquez sur **Appliquer** pour enregistrer la liste de surveillance et garder l'éditeur de liste de surveillance ouvert.
    - Cliquez sur **OK** pour enregistrer la liste de surveillance et fermer l'éditeur de liste de surveillance.
    - Cliquez sur **Annuler** pour fermer l'éditeur de liste de surveillance sans enregistrer vos modifications.

5.8.3. Importer une liste de surveillance

Les fonctions d'exportation et d'importation vous permettent de partager vos listes de surveillance et de recevoir celles de vos collègues. Importez des listes de surveillance existantes (fichiers *.csv) qui ont été enregistrées ou créées par UFED Physical Analyzer.

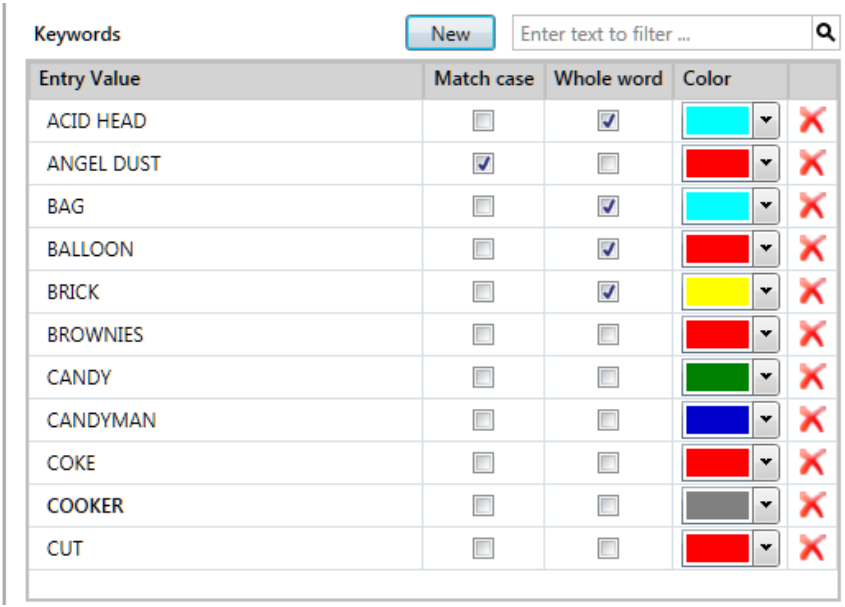
Vous pouvez également importer un fichier CSV qui contient une liste de mots clés, que vous pouvez ensuite utiliser comme mots clés de liste de surveillance. Cette option permet d'importer les mots clés sans formatage et recherche tous les types de données par défaut.

1) Dans la barre d'outils principale, cliquez sur .

   L'éditeur de liste de surveillance s'affiche.

2) Cliquez sur , et sélectionnez **Importer**.
3) Accédez à votre liste de surveillance, sélectionnez le fichier CSV, puis cliquez sur **Ouvrir**.

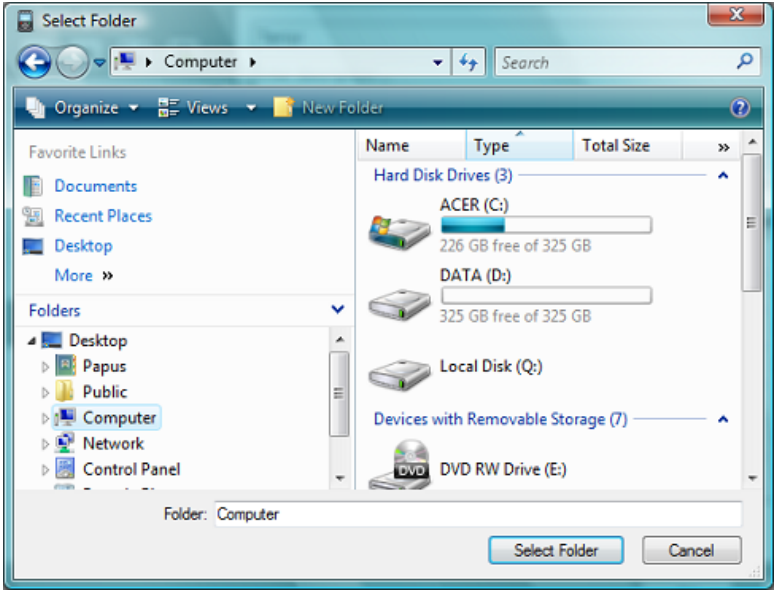
La liste de surveillance s'affiche dans l'éditeur de liste de surveillance. En voici un exemple :



5.8.4. Exporter une liste de surveillance

Exportez des listes de surveillance pour enregistrer une liste comme fichier *.csv, afin de la réutiliser ultérieurement ou de la partager avec d'autres personnes.

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez exporter.
2) Cliquez sur .

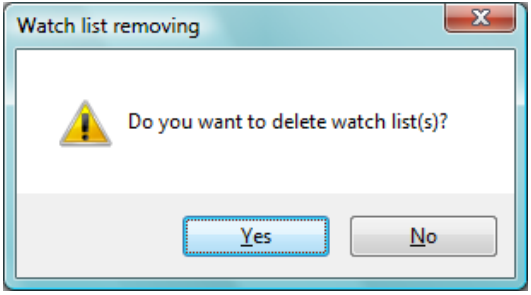


3) Accédez à l'emplacement dans lequel vous souhaitez enregistrer votre liste de surveillance, puis cliquez sur **Sélectionner dossier**.

   La liste de surveillance est exportée. Par défaut, elle est enregistrée comme [nom de la liste de surveillance].csv.

5.8.5. Supprimer une liste de surveillance

1) Dans l'éditeur de liste de surveillance, sélectionnez la liste que vous souhaitez supprimer.
2) Cliquez sur .



3) Cliquez sur **Oui**.

   La liste de surveillance est supprimée.

5.8.6. Exécuter une liste de surveillance

Vous pouvez exécuter des listes de surveillance sur les projets ouverts.

5.8.6.1. Exécuter une liste de surveillance sur des projets spécifiques

Lorsque vous exécutez une liste de surveillance depuis l'éditeur de liste de surveillance, vous pouvez sélectionner les listes à exécuter et sur quels projets vous souhaitez les exécuter.

1) Dans la barre d'outils, cliquez sur pour ouvrir l'éditeur de liste de surveillance, puis sélectionnez la liste que vous souhaitez exécuter.
2) Cliquez sur .

   Une liste des projets ouverts s'affiche.
3) Sélectionnez le ou les projets ouverts sur lesquels vous souhaitez exécuter la recherche.

   REMARQUE : Une coche ( ) indique que la liste de surveillance sélectionnée est active pour le projet.
4) Cliquez sur **Appliquer**.

   UFED Physical Analyzer recherche les mots-clés dans les projets sélectionnés. Une fois la recherche terminée, les résultats de la liste de surveillance s'affichent dans l'élément d'arborescence **Listes de surveillance**.

   Si la liste de surveillance est attribuée à des types d'informations spécifiques (voir ***Créer une liste de surveillance*** (page ***132***), seules les correspondances pour ces types s'affichent dans les résultats.

5.8.6.2. Exécuter une liste de surveillance sur votre projet en cours

Lorsque vous exécutez une liste de surveillance depuis l'arborescence de projet, vous pouvez sélectionner quelles listes exécuter pour le projet sur lequel vous êtes en train de travailler. Si plusieurs projets sont ouverts, les listes de surveillance sélectionnées s'exécutent sur le dernier projet sur lequel vous avez cliqué dans l'arborescence de projet.

1) Dans la barre d'outils, cliquez sur .

   Une liste des listes de surveillance s'affiche.

2) Sélectionnez la ou les listes de surveillance que vous souhaitez exécuter sur le projet en cours.

   REMARQUE : Une coche ( ) indique que la liste de surveillance est active pour le projet.

3) Cliquez sur **Appliquer** sur le projet mis en évidence dans l'arborescence de projet.

   REMARQUE : Lorsque vous cliquez sur dans la barre d'outils, vous ne pouvez exécuter les listes de surveillance que sur le dernier projet sur lequel vous avez cliqué dans l'arborescence de projet.

   UFED Physical Analyzer recherche les mots-clés dans les projets sélectionnés. Une fois la recherche terminée, les résultats de la liste de surveillance s'affichent dans l'élément d'arborescence **Listes de surveillance**.

Si la liste de surveillance est attribuée à des types d'informations spécifiques (voir ***Créer une liste de surveillance*** (page ***132***), seules les correspondances pour ces types s'affichent dans les résultats.

5.8.7. Localiser une liste de surveillance

1) Utilisez une des méthodes suivantes :
   - Dans la barre d'outils, cliquez sur .
   - Dans le menu **Outils**, sélectionnez **Éditeur de liste de surveillance**.

   L'éditeur de liste de surveillance s'affiche.
2) Dans la case **Saisir le texte à filtrer**, saisissez le nom (complet ou partiel) de la liste de surveillance, puis cliquez sur .
3) La liste des listes de surveillance est filtrée en conséquence.

5.9. Informations sur les signets (signets d'entités)

Un signet d'entité est un pointeur de référence rapide que vous pouvez créer pour des éléments individuels :

- Un élément de **Données analysées** tel qu'un appel du journal d'appels, un contact, un e-mail, etc. Consultez l'élément *Données analysées* dans la section ***Arborescence de projet*** (page ***76***).

- Un élément de **Fichiers de données** tel qu'un fichier image, un fichier vidéo, un fichier texte, etc. Consultez l'élément *Fichiers de données* dans la section ***Arborescence de projet*** (page ***76***).

Les signets d'entités que vous créez sont gérés dans l'élément **Signets d'entités** de l'arborescence. Le nombre de signets d'entités du projet apparaît entre parenthèses à côté du nom de la section.

- Double-cliquez sur **Signets d'entités** pour ouvrir une liste des signets d'entités dans un onglet dans la zone d'affichage des données. Les signets d'entité sélectionnés seront inclus dans les rapports générés.
- Double-cliquez sur un signet d'entité pour aller à l'élément marqué dans l'onglet d'affichage correspondant.

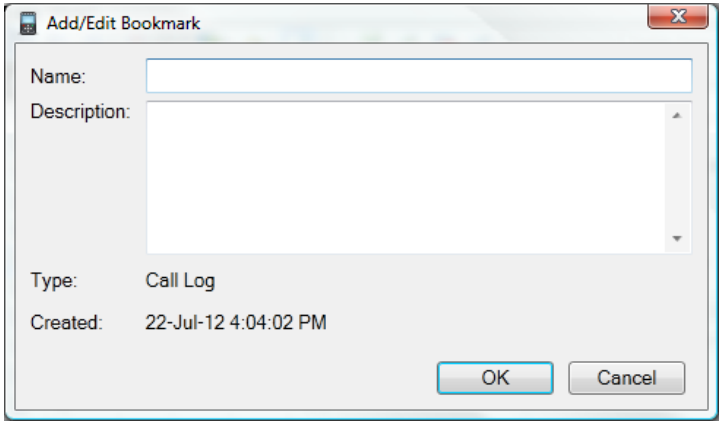
  Par exemple, double-cliquez sur un signet d'entité correspondant à un SMS pour ouvrir la liste de SMS dans un onglet d'affichage des Données analysées, avec l'élément marqué mis en surbrillance.
- Passez avec le curseur de la souris au-dessus d'un pour afficher le nom et la description du signet.
- Pour imprimer ou exporter uniquement la liste de signets d'entités, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Signets d'entités** : Excel , HTML , PDF ou XML .

5.9.1. Créer un nouveau signet d'entité

Vous pouvez ajouter des signets d'entités aux éléments de la vue Tableau.

1) Sélectionnez l'élément auquel vous voulez ajouter un signet.
2) Cliquez sur .

   La boîte de dialogue « Ajouter/modifier un signet » s'affiche.



3) Saisissez un nom et une description pour le nouveau signet d'entité, puis cliquez sur **OK**.

Un signet d'entité pointé vers l'élément sélectionné est ajouté à la liste de signets d'entités du projet. L'enregistrement d'élément marqué par un signet est indiqué par une bleue.

5.9.2. Modifier un signet d'entité

1) Choisissez une des options suivantes :
    - Un enregistrement de signet d'entité dans la liste des **Signets d'entités** de l'arborescence du projet.
    - Un élément marqué par un signet (indiqué par).
2) Cliquez sur dans la barre d'outils de la vue Tableau.

    La boîte de dialogue « Ajouter/modifier un signet » s'affiche.
3) Modifiez le nom ou la description, puis cliquez sur **OK**.

5.9.3. Supprimer un signet d'entité

1) Choisissez une des méthodes suivantes :
    - Un enregistrement de signet d'entité dans la liste des **Signets d'entités** de l'arborescence du projet.
    - Un élément marqué par un signet (indiqué par).
2) Cliquez sur dans la barre d'outils de la vue Tableau.

Le signet est supprimé.

5.10. Localisation des appareils

5.10.1. À propos des données de localisation

Dans UFED Physical Analyzer, les données de localisation sont extraites de plusieurs endroits dans l'appareil. Les données de localisation suivantes sont analysées :

Données analysées > **Localisations :**

Les données de localisation dans l'élément **Localisations** sont divisées en plusieurs catégories :

- Antennes relais téléphoniques
- Réseaux Wi-Fi
- Antennes relais téléphoniques récoltées
- Réseaux Wi-Fi récoltés
- Positions média

Informations de localisation récoltées et non récoltées :

Les informations de localisation récoltées et non récoltées sont tirées de la base de données de l'appareil.

La localisation de l'appareil est identifiée par les informations GPS de l'appareil, calculées de deux façons :

1) Collecte – Lorsque l'appareil se déplace avec son propriétaire, il collecte les informations de localisation de chaque antenne relais téléphonique et récepteur de réseau Wi-Fi dans son entourage. Ces localisations sont les informations « récoltées ». Les localisations calculées de cette façon sont considérées comme précises.

   Lorsque le Wi-Fi est activé sur l'appareil, celui-ci envoie régulièrement les localisations récoltées à Apple (appareils iPhone) ou Google (appareils Android). Les informations récoltées sont ensuite supprimées de l'appareil.

   Lorsque le Wi-Fi est désactivé sur l'appareil, ou en l'absence de connexion Wi-Fi disponible, l'appareil récolte et stocke les localisations des antennes relais téléphoniques et réseaux Wi-Fi, puis envoie les informations lorsque le Wi-Fi est activé ou qu'une connexion devient disponible.

2) Téléchargement – L'appareil se connecte au fournisseur de services de localisation (Apple pour les appareils iPhone ou Google pour les appareils Android), pour demander les services de localisation. Apple ou Google envoie les informations relatives aux antennes relais téléphoniques et aux réseaux Wi-Fi dans un rayon d'environ 2 kilomètres. Ces informations sont enregistrées sur l'appareil et sont appelées informations « non récoltées ».

Les données de localisation des catégories Antenne relais téléphoniques, Réseaux Wi-Fi, Antenne relais téléphoniques récoltées et Réseaux Wi-Fi récoltés incluent :

- Les informations GPS - longitude et latitude
- La précision - rayon en mètres dans lequel se trouve l'appareil.
- Confiance - en %. À quel point le fournisseur de service est certain que le téléphone se trouve bien à la position calculée.
- Horodatage

Positions média :

Les données de localisation dans **Positions média** sont extraites du tampon de localisation associé à chaque fichier multimédia.

Données analysées > Trajets :

Les données de localisation dans l'élément **Trajets** sont extraites des applications GPS sur l'appareil. Les catégories affichées dans cet élément sont divisées par application.

Données analysées > Références GPS :

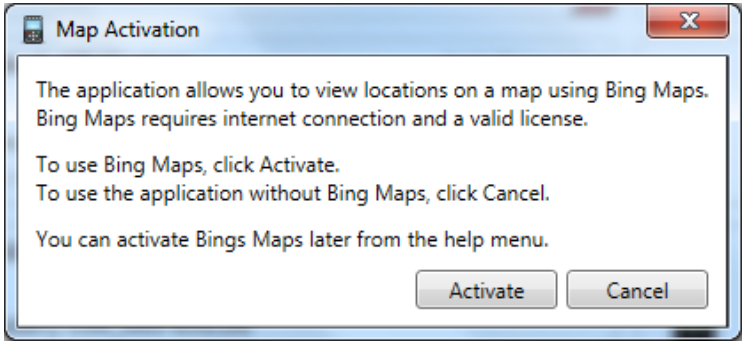
Les données de localisation dans l'élément **Références GPS** sont extraites des appareils GPS et des applications GPS sur l'appareil. Les catégories affichées dans cet élément sont divisées par application et par source.

5.10.2. Afficher les données de localisation sur BING

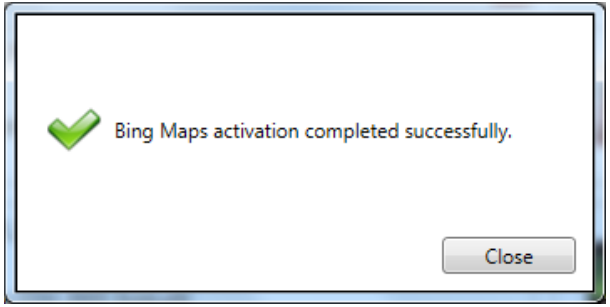
La fonction Cartes est gratuite mais nécessite un accès interne. Elle n'est disponible que pour les utilisateurs d'UFED Physical Analyzer qui disposent d'une licence valide.

Pour activer les cartes BING :

Lorsque vous démarrez UFED Physical Analyzer pour la première fois, vous êtes invité à activer vos cartes BING. L'écran suivant s'affiche :


Map Activation
The application allows you to view locations on a map using Bing Maps.
Bing Maps requires internet connection and a valid license.
To use Bing Maps, click Activate.
To use the application without Bing Maps, click Cancel.
You can activate Bings Maps later from the help menu.
Activate
Cancel

- Cliquez sur **Activer** pour activer vos cartes BING. Une fois l'activation effectuée, l'écran suivant s'affiche :



Si l'activation n'est pas effectuée au démarrage, il est possible d'activer les cartes Bing plus tard via le menu **Aide**.

Il est possible de parcourir et d'effectuer des recherches sur des cartes de rues topographiques de nombreuses villes dans le monde. Deux types de plan des rues sont disponibles : Vue routière, Vue aérienne.

Vue routière :

La vue routière est la carte par défaut. Elle affiche des images vectorielles des routes, des bâtiments et de la géographie.

Vue aérienne :

La vue aérienne superpose les images satellite à la carte et met en évidence les routes et les principaux repères pour une identification facile sur les images satellite.

5.10.3. Indicateurs et fenêtres d'informations

Les indicateurs marquent la position à laquelle l'appareil d'une personne est enregistré.

La couleur de l'indicateur montre quelle personne est enregistrée à une position particulière. À un faible niveau de zoom, les indicateurs montrent la position approximative et peuvent inclure les données de plusieurs personnes.

Les indicateurs suivants sont des exemples de ceux qui peuvent s'afficher sur une carte :

À un faible niveau de zoom, cet indicateur affiche plusieurs positions enregistrées dans une zone particulière.

Indique la position de l'antenne relai téléphonique qui a enregistré l'appareil de la personne.

Indique la position du récepteur de réseau Wi-Fi qui a enregistré l'appareil de la personne.

Indique la position enregistrée d'un objet multimédia.

Indique la position d'une entité non identifiée qui a enregistré l'appareil de la personne.

5.10.4. Récupération des adresses

Vous pouvez afficher les adresses pour obtenir la longitude et la latitude extraites d'un appareil. Cela peut être utile pour filtrer les localisations. Vous pouvez sélectionner une ou plusieurs localisations (jusqu'à 200). Vous pouvez récupérer les adresses dans les vues suivantes : Recherche de projet, vues Chronologie et Résultats de la liste de surveillance.

REMARQUE : Pour utiliser cette fonction, vous devez utiliser le service de cartes Bing et être connecté à Internet.

Pour récupérer une adresse :

1) Dans l'un des affichages par tableau des localisations de l'appareil, sélectionnez une ligne, faites un clic droit et sélectionnez **Récupérer l'adresse**, ou cliquez sur .

REMARQUE : Pour récupérer plusieurs adresses, vous pouvez utiliser la touche Ctrl afin de sélectionner les localisations souhaitées.

	Timestamp	Position	Map Address
	1/25/2011 3:29:27 PM(UTC+0)	(46.244610, -70.801400)	Beauceville, QC, Canada
	1/25/2011 2:29:00 PM(UTC+0)	(46.779900, -71.267570)	
	1/25/2011 1:20:30 PM(UTC+0)	(46.788060, -71.281680)	787 Avenue Nérée-Tremblay, Quebec, QC G1V 4K3, Canada
	1/25/2011 12:19:45 PM(UTC+0)	(46.788470, -71.282010)	
	1/25/2011 11:16:02 AM(UTC+0)	(46.803410, -71.231840)	330 Rue Père-Marquette, Québec, QC G1S 1Y8, Canada
	1/25/2011 10:15:08 AM(UTC+0)	(46.778810, -71.261080)	2186 Rue Brulart, Quebec, QC G1T 1G4, Canada

Les adresses récupérées sont affichées en rouge dans la colonne nommée « Adresse sur la carte ».

Pour filtrer les localisations :

- Cliquez sur , puis sélectionnez l'une des options suivantes :
  - **Afficher tout** pour afficher toutes les localisations.
  - **Avec adresse sur la carte** pour afficher les localisations qui possèdent une adresse sur la carte.
  - **Sans adresse sur la carte** pour afficher les localisations qui ne possèdent pas d'adresse sur la carte.

Chapitre 6 : **Traduction de données décodées**

Traduisez le contenu de vos extractions en langue étrangère sans attendre qu'un traducteur soit disponible, ni utiliser d'outils en ligne.

La fonction Traduction permet de traduire les données décodées sur demande, pour permettre aux enquêteurs de comprendre les informations disponibles dans une extraction. La fonction Traduction est une solution de traduction hors connexion, qui ne nécessite pas d'être connecté à Internet. Vous pouvez sélectionner une, plusieurs ou toutes les entrées du tableau pour les traduire. Le texte d'origine et le texte traduit peuvent être inclus dans le rapport.

Les langues prises en charge sont les suivantes :

Chinois (simplifié)
Chinois (traditionnel)
Néerlandais
Allemand
Hébreu
Italien
Français
Japonais (payant)
Coréen
Polonais
Portugais
Russe
Espagnol
Ukrainien

6.1. Utilisation de la fonction

Pour utiliser cette fonction, procédez de la façon suivante :

- Mettez à jour votre licence avec les langues sélectionnées.
- Téléchargez le package de traduction.
- Traduisez les données décodées.

6.2. Mettre à jour votre licence avec les langues sélectionnées

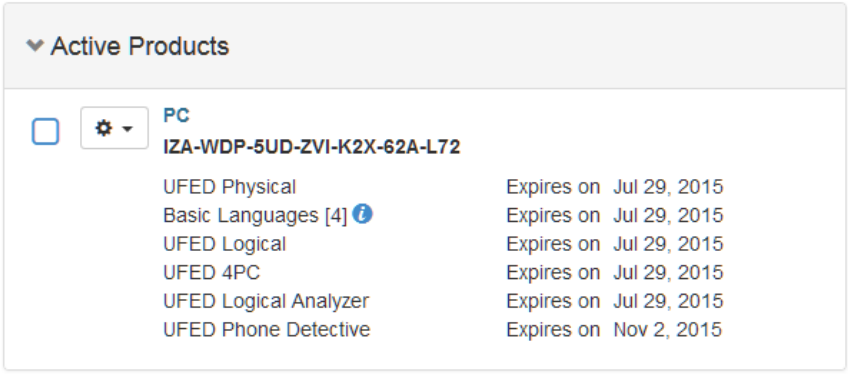
Vous pouvez sélectionner jusqu'à cinq langues gratuitement sur la page Mes produits dans MyCellebrite. Si vous avez besoin de langues supplémentaires, vous pouvez acheter le Pack Langue basique. Vous ne pouvez pas modifier une langue après l'avoir enregistrée, mais vous pouvez demander des langues supplémentaires.

REMARQUE : Si vous souhaitez effectuer la traduction vers une langue autre que l'anglais, vous devez également la sélectionner.

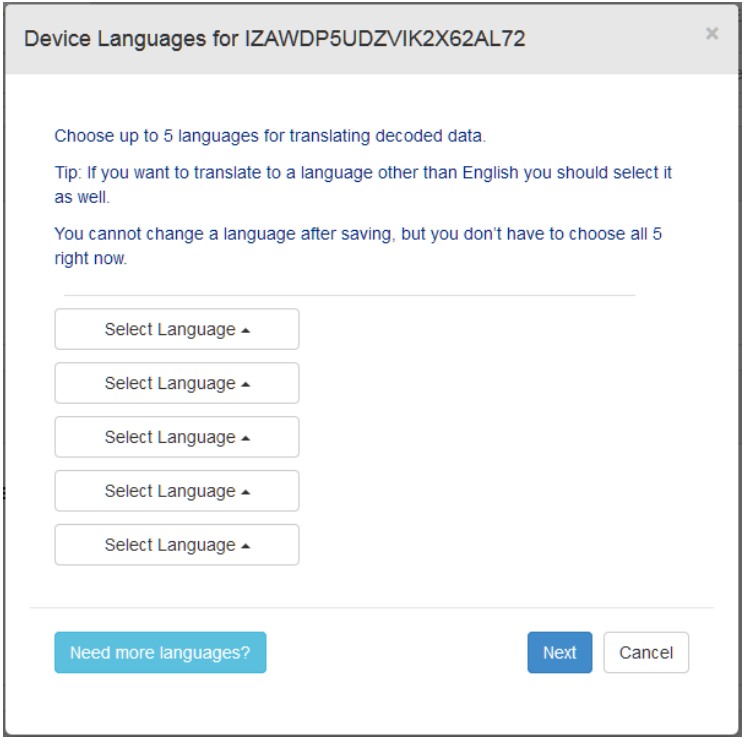
6.2.1. Sélectionner des langues dans MyCellebrite

Pour sélectionner des langues :

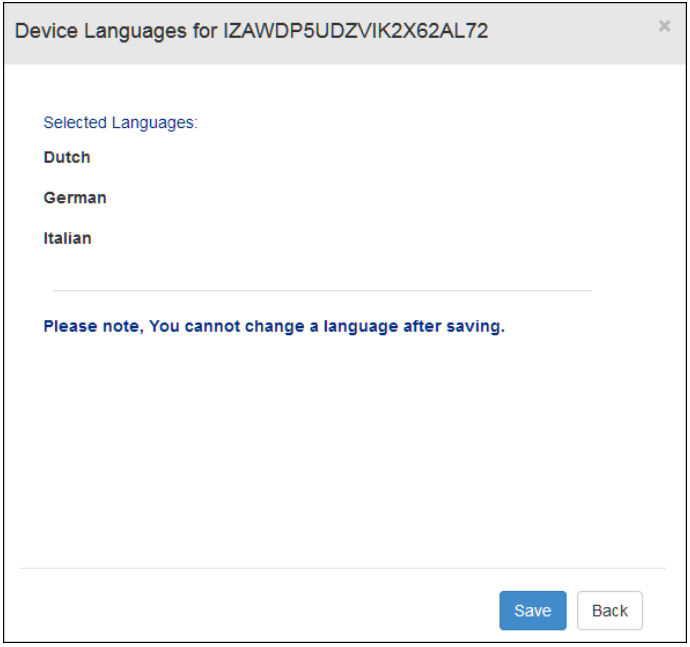
1) Connectez-vous à MyCellebrite et sélectionnez l'onglet **Mes produits**. La fenêtre suivante s'affiche :


Active Products
PC
IZA-WDP-5UD-ZVI-K2X-62A-L72
UFED Physical Expires on Jul 29, 2015
Basic Languages [4] Expires on Jul 29, 2015
UFED Logical Expires on Jul 29, 2015
UFED 4PC Expires on Jul 29, 2015
UFED Logical Analyzer Expires on Jul 29, 2015
UFED Phone Detective Expires on Nov 2, 2015

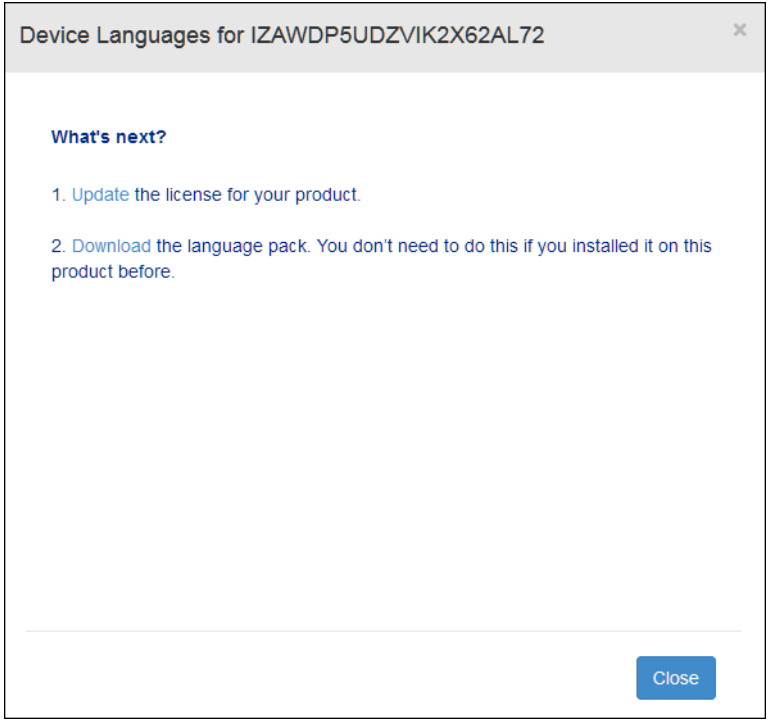
2) Sélectionnez , puis cliquez sur **Sélectionner les langues**. La fenêtre suivante s'affiche :


Device Languages for IZAWDP5UDZVIK2X62AL72
Choose up to 5 languages for translating decoded data.
Tip: If you want to translate to a language other than English you should select it as well.
You cannot change a language after saving, but you don't have to choose all 5 right now.
Select Language
Select Language
Select Language
Select Language
Select Language
Need more languages?
Next
Cancel

3) Sélectionnez jusqu'à cinq langues de traduction, puis cliquez sur **Suivant**. La fenêtre suivante s'affiche : Pour des langues supplémentaires, cliquez sur **Besoin de langues supplémentaires** et remplissez le formulaire.



4) Cliquez sur **Enregistrer**. La fenêtre suivante s'affiche :


Device Languages for IZAWDP5UDZVIK2X62AL72
What's next?
1. Update the license for your product.
2. Download the language pack. You don't need to do this if you installed it on this product before.
Close

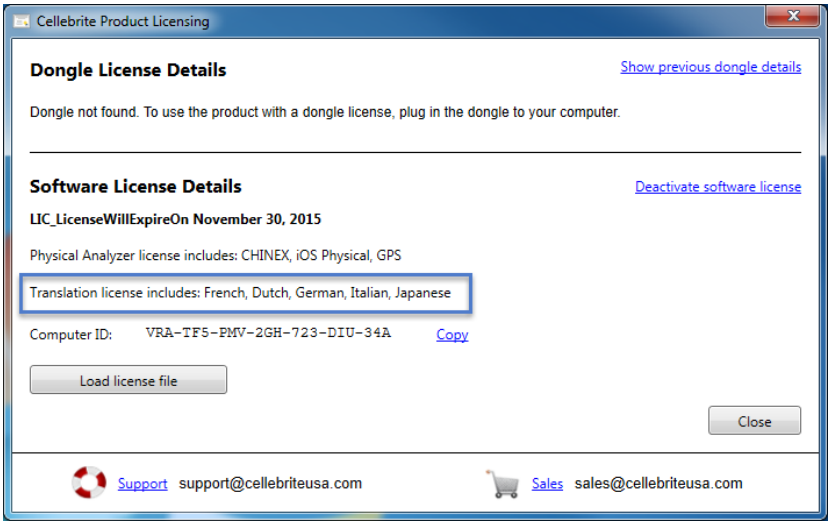
5) Mettez à jour la licence pour le produit, puis téléchargez le package de langues.

Une fois votre licence produit mise à jour avec les langues sélectionnées, suivez la procédure ci-dessous pour afficher les langues incluses dans la licence de traduction.

Pour consulter les langues de la licence de traduction :

- Sélectionnez **Outils > Traduction > Afficher les langues prises en charge**.

  L'écran suivant s'affiche :


Cellebrite Product Licensing
Dongle License Details
Show previous dongle details
Dongle not found. To use the product with a dongle license, plug in the dongle to your computer.
Software License Details
Deactivate software license
LIC_LicenseWillExpireOn November 30, 2015
Physical Analyzer license includes: CHINEX, iOS Physical, GPS
Translation license includes: French, Dutch, German, Italian, Japanese
Computer ID: VRA-TF5-PMV-2GH-723-DIU-34A
Copy
Load license file
Close
Support support@cellebriteusa.com
Sales sales@cellebriteusa.com

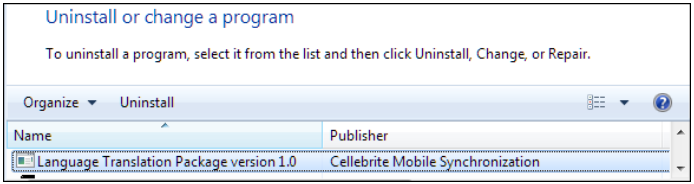
6.2.2. Téléchargez le package de traduction

Vous pouvez télécharger le package de traduction depuis l'application ou depuis votre compte my.cellebrite.com. Le package de traduction inclut un numéro de version, qui vous permet de suivre la version installée sur l'ordinateur.

Pour télécharger le package de traduction :

1) Sélectionnez **Outils** > **Traduction.**
2) Choisissez l'une des options suivantes :
    - **Télécharger le package de traduction :** Télécharge le package de traduction (cette option n'est pas disponible si vous n'êtes pas connecté à Internet).
    - **Installer le package de traduction à partir d'un fichier :** Installe le package de traduction à partir d'un fichier. Sélectionnez cette option si vous n'êtes pas connecté à Internet.
3) Suivez les instructions à l'écran pour installer le package de traduction.

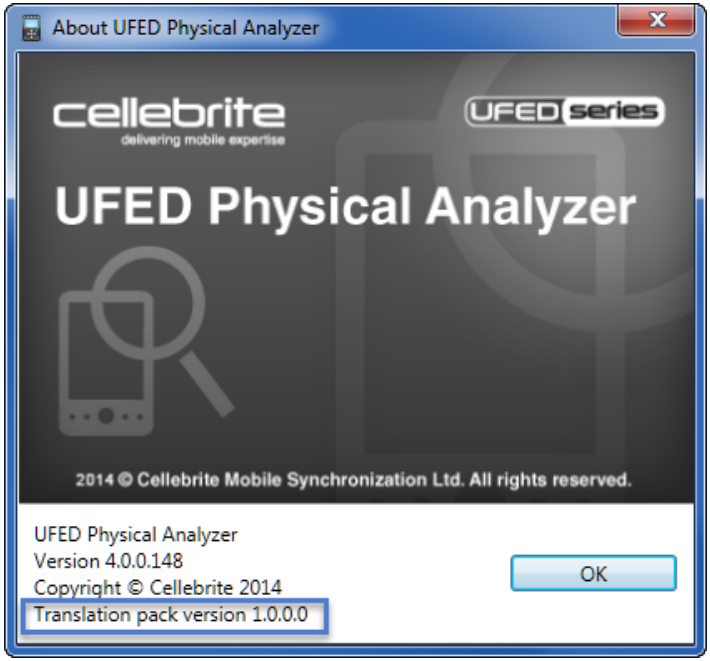
REMARQUE : Pour désinstaller le package de traduction, rendez-vous sur la page Désinstaller de Windows, et sélectionnez le package de traduction des langues (Publisher : Cellebrite Mobile Synchronization) dans la liste.


Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Uninstall
Name
Publisher
Language Translation Package version 1.0
Cellebrite Mobile Synchronization

Pour afficher le numéro de version du package de traduction :

- Cliquez sur **Aide** > **À propos**.

  L'écran suivant s'affiche :



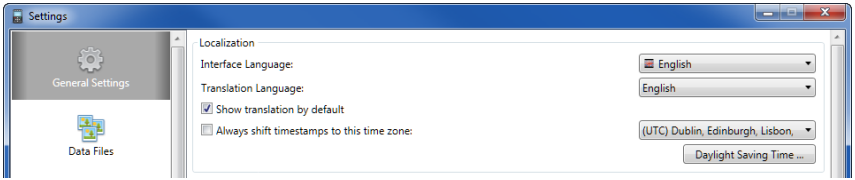
6.2.3. Traduction de données décodées

Par défaut, la langue cible définie est la même que la langue de l'interface. Si nécessaire, vous pouvez choisir une langue cible différente.

Pour modifier la langue de traduction :

1) Sélectionnez **Outils** > **Paramètres.**

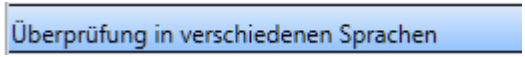
   L'écran suivant s'affiche :



2) Sélectionnez la langue de traduction. C'est la langue dans laquelle vous souhaitez traduire le texte. Vous ne pouvez sélectionner qu'une seule langue de traduction. Pour demandez des langues de traduction supplémentaires, sélectionnez **Plus de langues**.
3) Cochez la case **Afficher la langue de traduction par défaut** pour afficher les traductions par défaut. Décochez cette case pour que la traduction n'apparaisse pas lorsque vous traduisez le texte. Pour afficher la traduction, sélectionnez **Afficher la traduction**.

Pour traduire des données décodées :

1) Cliquez sur les données que vous souhaitez traduire pour les sélectionner.



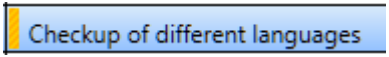
2) Cliquez sur le bouton

ou sur le bouton droite de la souris et sélectionnez **Traduire la sélection**, ou cliquez sur , puis sélectionnez l'une des options suivantes :

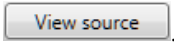
- **Traduire tout :** Traduit toutes les entrées dans le champ spécifié.
- **Traduire la sélection :** Traduit uniquement le texte sélectionné.

REMARQUE : Si nécessaire, utilisez l'option **Supprimer la traduction** pour supprimer le texte traduit.

Le texte traduit est indiqué par une barre jaune.

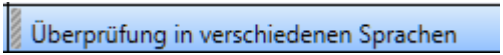


Pour afficher le texte source :

1) Cliquez avec le bouton droit de la souris sur le texte et sélectionnez **Afficher la source**, ou cliquez sur le bouton 

.

Le texte source est indiqué par une barre grise.



Pour filtrer le texte :

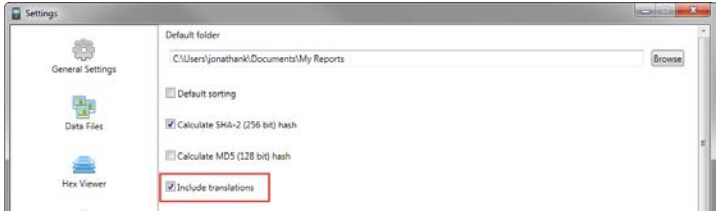
- Cliquez sur , puis sélectionnez l'une des options suivantes :
    - **Tout** pour afficher tout le texte.
    - **Traduit** pour afficher le texte traduit.
    - **Non traduit** pour afficher le texte non traduit.

6.2.4. Reporting

Lors de la création de rapports ou de l'exportation de données, vous pouvez préciser si vous souhaitez inclure le texte traduit ou non. Si vous choisissez d'afficher le texte traduit dans le rapport, le tableau de résumé inclut une entrée supplémentaire nommée : Langues traduites, avec une liste des langues. Le contenu traduit apparaît en-dessous du texte source, sous l'en-tête : Traduction. Pour plus d'informations sur les rapports, consultez la section Générer un rapport, page *187*.

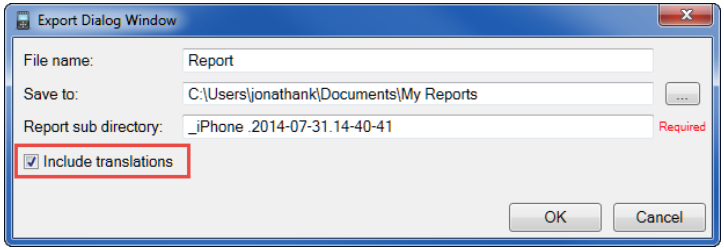
Pour inclure le texte traduit dans les rapports :

1) Allez dans **Outils** > **Paramètres** > **Paramètres généraux** > **Paramètres par défaut pour du rapport**.
2) Cochez la case **Inclure les traductions**.



Pour inclure le texte traduit dans les exportations :

1) Cliquez sur une option d'exportation ( ).
2) Cochez la case **Inclure les traductions**.



Chapitre 7 : **Travailler avec l'analyse de projet**

L'analyse de projet vous permet de visualiser les données de l'extraction en termes de nombre d'événements de communication entre l'appareil et d'autres parties, identifiées selon leur numéro de téléphone ou d'autres identifiants utilisateur (adresse e-mail, identifiant Skype, etc.). L'analyse vous permet d'identifier facilement et efficacement les schémas de communication entre l'appareil et les autres parties. Par exemple :

- Les parties avec lesquelles l'appareil communique le plus, via tous types de méthodes de communication ;
- Les parties avec lesquelles l'appareil communique le plus, via appels téléphoniques, SMS et MMS.

Si l'utilisateur de l'appareil a échangé un grand nombre d'appels téléphoniques, SMS et e-mails avec un certain contact, il est facile de voir le volume de ces communications.

Les événements de communication sont répertoriés par volume et par type. Les événements de communication suivants sont pris en charge :

- **Téléphones** – répertorie les appels sortants, entrants et manqués, et les SMS et MMS envoyés et reçus, ainsi que les brouillons.
- **E-mails** – répertorie les e-mails envoyés, reçus, les brouillons et les e-mails de statut inconnu.
- **WhatsApp** – répertorie les messages envoyés, reçus et les brouillons.

- **Skype** – répertorie les appels, SMS et les messages instantanés.
- **BlackBerry Messenger** – répertorie les messages instantanés.

L'analyse du projet s'exécute automatiquement lorsque vous ouvrez un fichier d'extraction.

Pour afficher l'analyse de projet :

1) Cliquez sur ⊞ à côté de l'élément d'arborescence **Analyse du projet** pour afficher les résultats de l'analyse dans l'élément d'arborescence **Analyse du projet**.
2) Double-cliquez sur l'élément d'arborescence **Analyse du projet** pour ouvrir un onglet qui affiche les cinq activités les plus importantes par contact.
3) Pour afficher une vue d'ensemble comparative de tous les événements de communication, double-cliquez sur l'élément d'arborescence **Analyse de l'activité**. La vue est triée par ordre croissant, en fonction du nombre total d'événements.

4) Pour afficher les événements par identifiant de communication, double-cliquez sur l'élément d'arborescence de l'identifiant souhaité.
5) Cliquez sur l'en-tête d'une colonne pour trier les informations dans celle-ci.

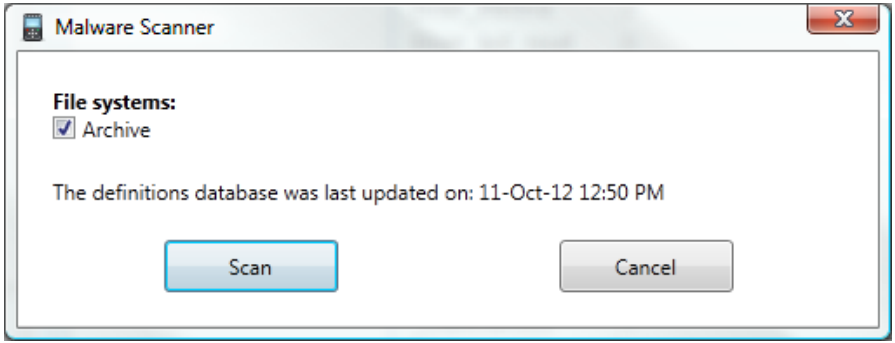
REMARQUE : Les informations de l'analyse de projet peuvent être incluses dans un rapport. Pour en savoir plus, consultez la section Générer un rapport.

Chapitre 8 : **Rechercher les malware**

Exécutez la détection de malware sur votre extraction pour rechercher les malware.

Lors d'une recherche de malware, UFED Physical Analyzer utilise la dernière base de données de signature utilisée. Si vous utilisez le scanner anti-malware pour la première fois, ou si vous souhaitez mettre à jour la base de données avant d'effectuer le scan, suivez les étapes décrites dans la section ***Mettre à jour la base de données de signature (en ligne)*** (page ***178***). Si vous travaillez sur un ordinateur sans connexion Internet, suivez les étapes décrites dans la section ***Mettre à jour la base de données de signature depuis un fichier (hors connexion)*** (page ***180***).

1) Sélectionnez **Outils** > **Scanner anti-malware** > **Rechercher les malware** ou cliquez sur .



2) Sélectionnez le ou les systèmes que vous voulez scanner, puis cliquez sur **Scan**.

   UFED Physical Analyzer recherche les malware dans le projet. Les résultats sont affichés dans l'élément d'arborescence **Scanner anti-malware**.

3) Double-cliquez sur l'élément d'arborescence **Scanner anti-malware** pour ouvrir un onglet d'affichage des données.

   Les données affichées incluent le type de malware et les informations correspondantes, telles que le nom du malware.

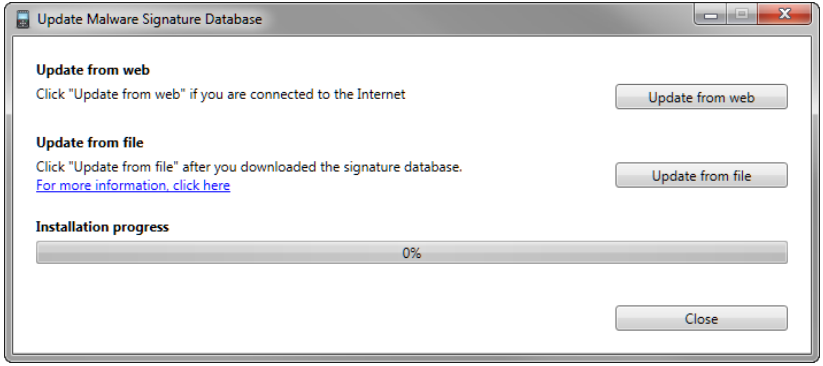
- Pour inclure les résultats dans un rapport, sélectionnez **Fichiers infectés** dans la zone **Ensemble de données du rapport**. Pour plus d'informations, consultez la section ***Générer un rapport***.

8.1. Mettre à jour la base de données de signature (en ligne)

Mettez à jour la base de données de signature avant d'utiliser le scanner anti-malware pour la première fois, afin de remplir la base de données, et ensuite afin de maintenir la base de données de signature à jour.

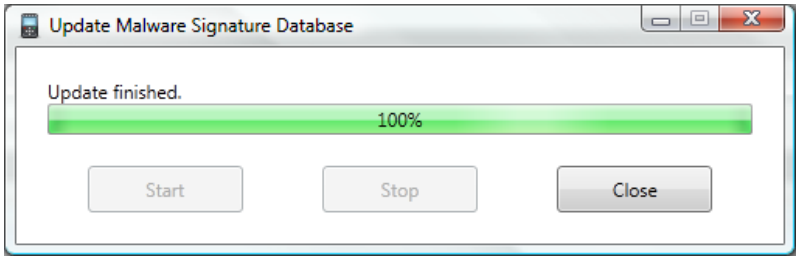
REMARQUE : Une fois la base de données de signature remplie, vous pouvez exécuter le scanner anti-malware en utilisant la base de données existante. Il est fortement conseillé de mettre à jour la base de données de signature régulièrement afin qu'elle reste à jour.

1) Dans le menu **Outils**, sélectionnez **Scanner anti-malware** > **Mettre à jour la base de données de signature**.


Update Malware Signature Database
Update from web
Click "Update from web" if you are connected to the Internet
Update from web
Update from file
Click "Update from file" after you downloaded the signature database.
For more information, click here
Update from file
Installation progress
0%
Close

2) Cliquez sur **Mettre à jour depuis le serveur**.

La base de données est remplie.



3) Cliquez sur **Fermer**.

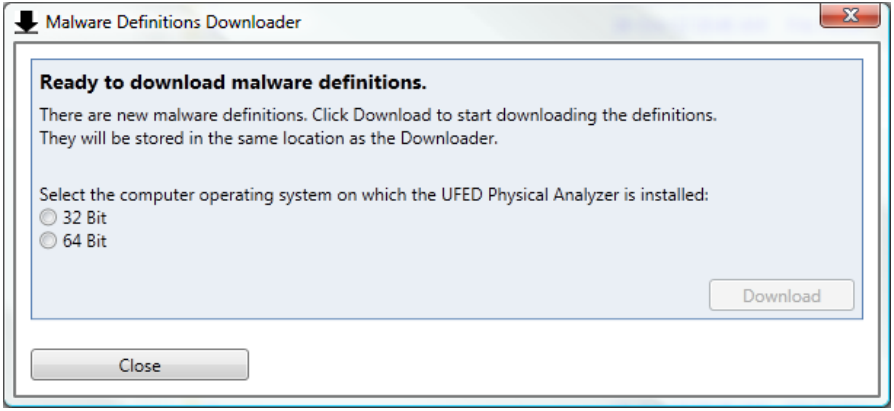
Vous pouvez maintenant scanner le projet pour rechercher des malware.

8.2. Mettre à jour la base de données de signature depuis un fichier (hors connexion)

Mettez à jour la base de données de signature à partir d'un fichier lorsque vous travaillez sur un ordinateur qui n'est pas connecté à Internet.

REMARQUE : Une fois la base de données de signature remplie, vous pouvez exécuter le scanner anti-malware en utilisant la base de données existante. Il est fortement conseillé de mettre à jour la base de données de signature régulièrement afin qu'elle reste à jour.

1) Dans Windows Explorer, dans le répertoire principal de UFED Physical Analyzer, copiez le répertoire **BitDefenderUpdater** sur un dispositif de stockage externe.
2) Transférez le répertoire **BitDefenderUpdater** sur un ordinateur connecté à Internet sans paramètres Proxy.
3) Dans le répertoire **BitDefenderUpdater**, double-cliquez sur **Malware Definitions Downloader.exe**.


Malware Definitions Downloader
Ready to download malware definitions.
There are new malware definitions. Click Download to start downloading the definitions.
They will be stored in the same location as the Downloader.
Select the computer operating system on which the UFED Physical Analyzer is installed:
32 Bit
64 Bit
Download
Close

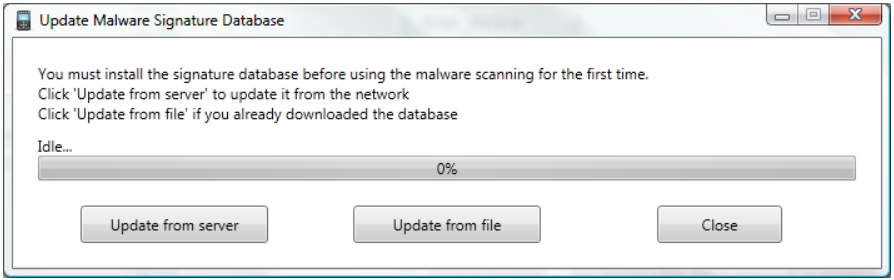
4) Sélectionnez le système d'exploitation de l'ordinateur sur lequel UFED Physical Analyzer est installé.
5) Cliquez sur **Télécharger**.

Malware Definitions Downloader
Download completed successfully!
Copy the definitions file to a storage device (if it's not already on one), connect it back to the computer running Physical Analyzer and continue there.
Open containing folder
Close

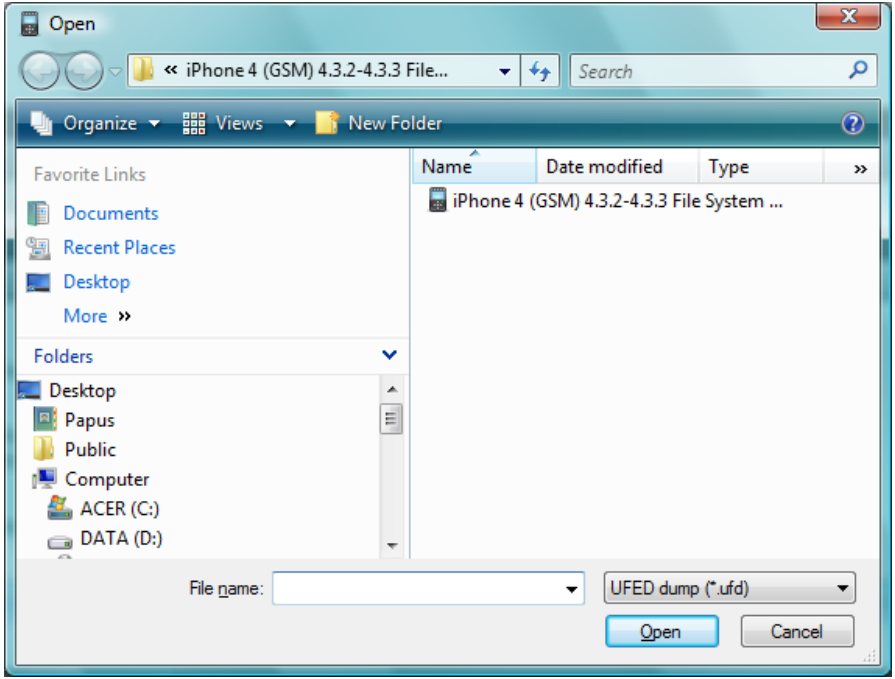
6) Cliquez sur **Ouvrir le dossier**.
7) Copiez le fichier **definitions.msd** sur un dispositif de stockage externe, puis transférez-le sur l'ordinateur sur lequel UFED Physical Analyzer est installé.
8) Cliquez sur **Fermer** pour fermer le programme de téléchargement des définitions de malware.

REMARQUE : Pour simplifier votre travail et gagner du temps, il est conseillé d'utiliser toujours le même ordinateur pour télécharger le fichier **definitions.msd**. Lorsque vous téléchargerez le fichier **definitions.msd** sur cet ordinateur à l'avenir, le programme de téléchargement des définitions de malware mettra à jour le fichier au lieu de le télécharger en totalité. Assurez-vous de ne pas supprimer le fichier **definitions.msd** de cet ordinateur.

9) Dans UFED Physical Analyzer, sélectionnez **Outils** > **Scanner anti-malware** > **Mettre à jour la base de données de signature**.

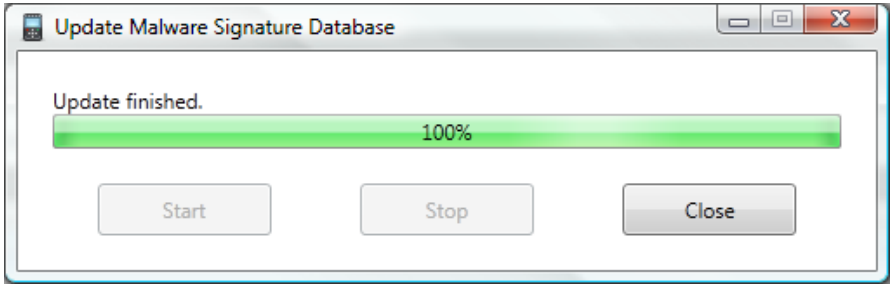

Update Malware Signature Database
You must install the signature database before using the malware scanning for the first time.
Click 'Update from server' to update it from the network
Click 'Update from file' if you already downloaded the database
Idle...
0%
Update from server
Update from file
Close

10) Cliquez sur **Mettre à jour depuis le fichier**.



11) Accédez à au fichier de base de données de définitions des malware (*.msd), puis cliquez sur **Ouvrir**.
12) Cliquez sur **Démarrer**.

La base de données est remplie.



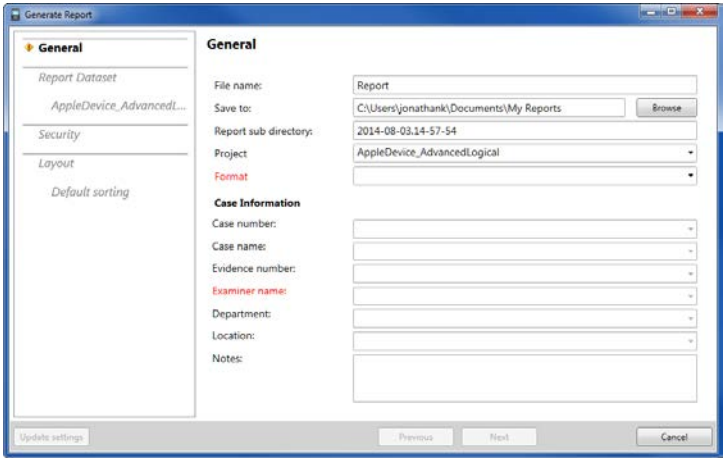
13) Cliquez sur **Fermer**.

Vous pouvez maintenant scanner le projet pour rechercher des malware.

Chapitre 9 : **Générer un rapport**

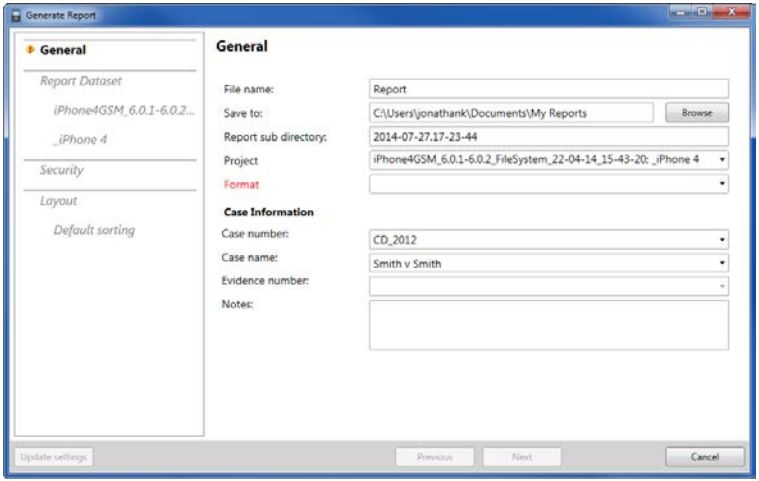
1) Vous pouvez générer un rapport contenant les informations du projet. UFED Physical Analyzer fournit un assistant de création de rapport qui vous aide tout au long des étapes de la création d'un rapport. Utilisez une des méthodes suivantes :
    - Sélectionnez **Rapport** > **Générer un rapport** dans le menu de l'application.
    - Cliquez sur **Générer un rapport** dans l'onglet **Résumé d'extraction**.
    - Double-cliquez sur **Rapports** dans l'arborescence de projet.

L'écran Générer un rapport s'affiche.

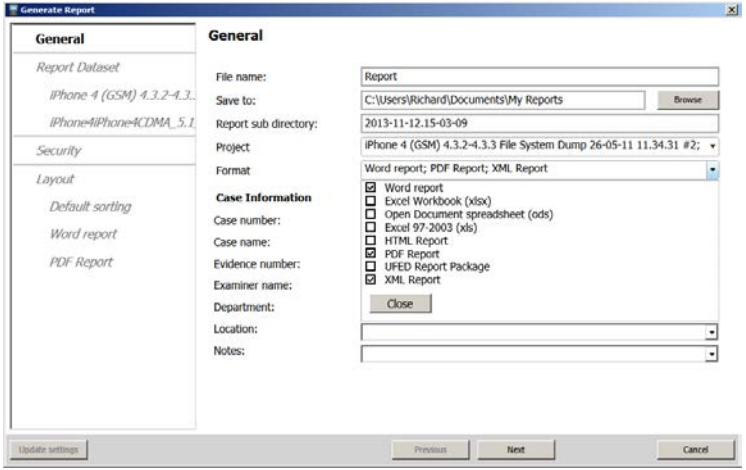


2) Dans **Nom de fichier**, sélectionnez le nom du nouveau rapport que vous souhaitez créer.
3) Dans **Enregistrer sur**, sélectionnez le dossier dans lequel vous souhaitez que tous les rapports soient créés. Ce dossier peut être utilisé pour tous les rapports, car chacun sera placé dans un sous-dossier distinct.
4) Dans **Sous-répertoire du rapport**, sélectionnez un nom pour le dossier dans lequel vous souhaitez que tous les rapports sélectionnez soient créés. Par défaut, ce nom est composé de la date et l'heure actuelles.

5) Dans **Projet**, sélectionnez le ou les projets que vous souhaitez inclure dans ce rapport. Seuls les projets déjà ouverts dans UFED Physical Analyzer peuvent être sélectionnés pour créer un rapport.



6) Dans le champ « Format », choisissez le format souhaité pour le rapport. Il est possible de sélectionner plusieurs formats. Dans ce cas, un rapport est créé pour chaque format.

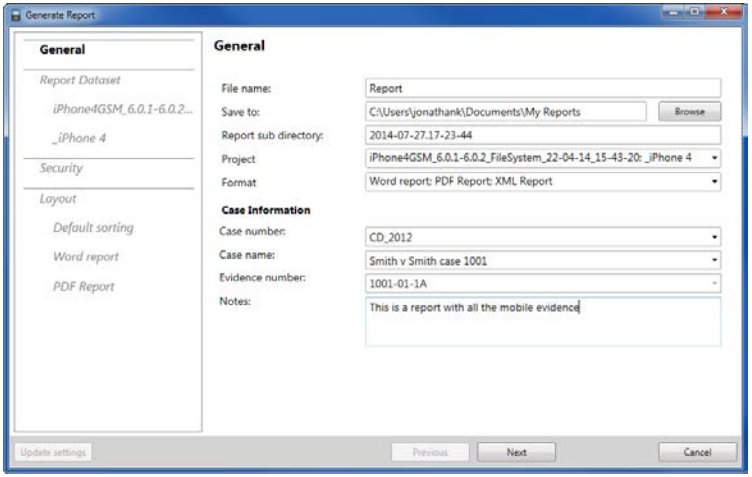


7) Pour les champs « Informations sur le cas », vous pouvez fournir les informations suivantes :

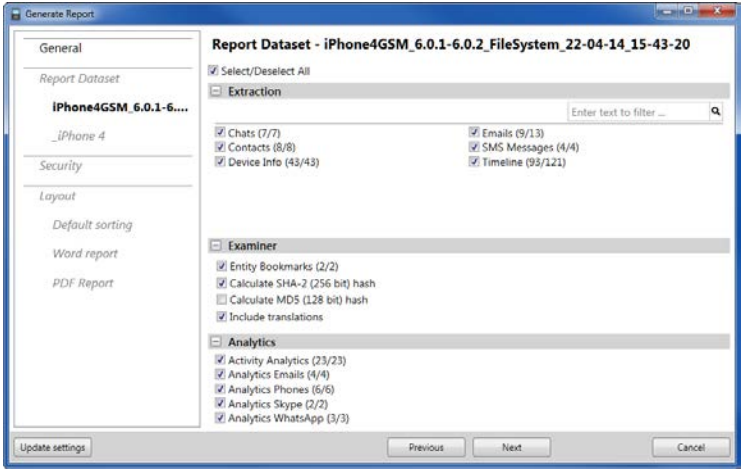
- **Numéro de cas**
- **Nom du cas**
- **Numéro de preuve**
- **Nom examinateur**
- **Service**
- **Lieu**

REMARQUE : Paramètres par défaut pour ces champs. Consultez la section ***Définir les informations du dossier*** (page ***376***). Consultez les sections ***Champs de rapport supplémentaires*** (page ***356***) et ***Paramètres par défaut du rapport*** (page ***359***) pour obtenir des paramètres par défaut supplémentaires. En outre, les 10 dernières valeurs saisies dans ces champs sont également disponibles dans la liste déroulante.

8) Votre formulaire doit alors ressembler à l'exemple ci-dessous :



9) Dans l'écran suivant, sélectionnez les données à inclure dans le rapport.



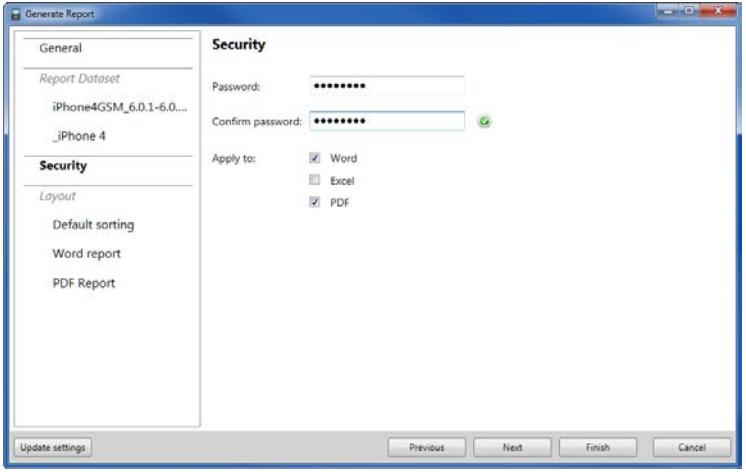
a) **Extraction** – données analysées et fichiers de données à inclure dans le rapport.

b) **Examinateur** – **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** - sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Cette sélection concerne l'ensemble du rapport et s'applique à tous les projets contenus dans le rapport. CONSEIL : Pour raccourcir le processus de création de rapports pour les projets importants, ne sélectionnez pas ces options.

Sélectionnez **Inclure les traductions** pour inclure le texte traduit. Le tableau de résumé inclut alors une entrée supplémentaire, Langues traduites, et la traduction du contenu apparaît sous le texte source avec le titre Traduction.

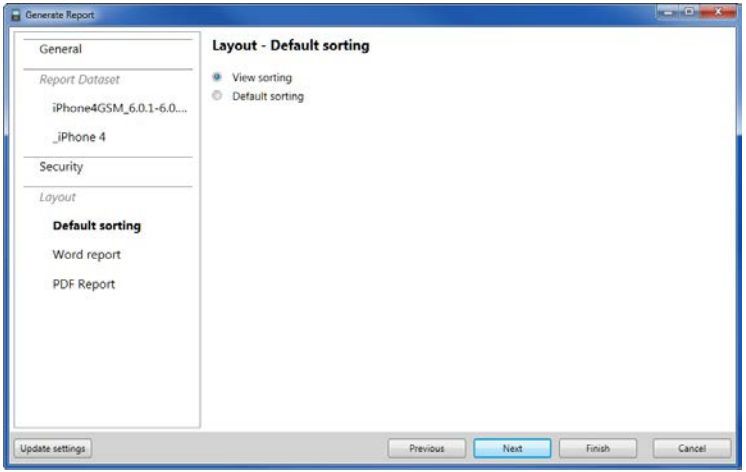
c) **Analyse** – cette section apparaît lorsque l'élément d'arborescence **Analyse** est disponible dans le projet. Sélectionnez les éléments d'analyse concernés pour les inclure dans le rapport.

10) L'écran **Sécurité** s'affiche. Les rapports au format PDF, Word et Excel peuvent être protégés par mot de passe :



Choisissez le format et saisissez un mot de passe.

11) Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.



12) Pour chaque format choisi pour ce rapport, vous pouvez préciser les paramètres de rapport de la façon suivante :

    a) Rapports au format Word, HTML et PDF :

    - **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).
    - **En-tête du logo** – zone de texte dans laquelle vous pouvez saisir et personnaliser le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
    - **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
    - **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
    - **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
    - **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette

option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.

- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par chat** – définit le nombre maximum de messages affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.
- **Famille de police** – pour les rapports au format PDF uniquement.
- **Diviser le rapport HTML** – pour les rapports au format HTML uniquement. Garantit que chaque section du rapport commence sur une nouvelle page.

b) Rapports au format Excel (tous formats) et ODS :

- **Rapport Excel compatible avec OpenOffice** – sélectionnez cette option pour vous assurer que le rapport Excel pourra être ouvert sous OpenOffice.
- **Générer les données d'identification du contact** – sélectionnez cette option pour ajouter une feuille au rapport Excel contenant une liste des contacts uniques en fonction du type.

c) Package de rapport UFED et XML :

- AUCUN paramètre supplémentaire n'est requis pour ces rapports. Si les formats de rapport demandés incluent uniquement des rapports XML et/ou UFED, aucune information supplémentaire n'est nécessaire.

13) Cliquez sur **Terminer**.

REMARQUE : L'option **Terminer** ne devient disponible qu'une fois que les champs obligatoires sont remplis. Une icône d'avertissement jaune s'affiche à côté de tous les champs requis qui ne sont pas remplis.

Lorsque le rapport a bien été créé, vous êtes invité à ouvrir le fichier correspondant. Celui-ci s'ouvre avec l'application correspondant au format de fichier installée sur le poste de travail.

Une fois qu'un rapport été créé pour le projet, il est accessible dans la section Rapports de l'arborescence de projet. Double-cliquez sur le rapport de votre choix pour l'ouvrir avec l'application correspondante installée sur le poste de travail. Cliquez avec le bouton droit de la souris sur un rapport généré pour ouvrir le fichier du rapport, ou sélectionnez **Ouvrir le dossier** pour parcourir les fichiers et dossiers du rapport.

Chapitre 10 : **Effectuer des extractions**

Dans UFED Physical Analyzer, utilisez l'une des méthodes suivantes pour effectuer des extractions d'appareils :

1) Pour les appareils iOS, l'extraction numérique avancée, l'extraction physique, l'extraction de système de fichiers ou la récupération de mot de passe de l'appareil s'effectuent au moyen de l'application iOS Device Extraction.
2) Pour le GPS ou le stockage de masse, l'extraction s'effectue via UFED Physical Analyzer.

10.1. Extraction d'appareils iOS

Pour effectuer une extraction physique ou une extraction numérique avancée d'un appareil iPhone, iPod ou iPad, utilisez iOS Device Extraction.

10.1.1. Conditions préalables

Pour effectuer une extraction depuis un appareil iOS, il vous faut :

- UFED Physical Analyzer installé sur un PC ;

- Un câble UFED n°110, un câble A UFED avec embout T-110 ou un câble USB à 30 broches Apple, fournis avec l'appareil ;
- Un câble UFED n°210 pour les extractions numériques iOS depuis un iPhone 5, un iPad Mini et un iPad4.

REMARQUE : L'extraction d'appareils iOS n'est pas compatible avec les environnements de la machine virtuelle.

En outre, une connexion Internet est nécessaire lors de la première exécution d'iOS Device Extraction afin de télécharger le pack correctif nécessaire. Vous pouvez également télécharger le pack correctif sur un autre ordinateur et le copier manuellement sur l'ordinateur utilisant iOS Device Extraction. iOS Device Extraction vous avertit automatiquement lorsqu'une mise à jour logicielle est disponible.

10.1.2. Effectuer une extraction physique

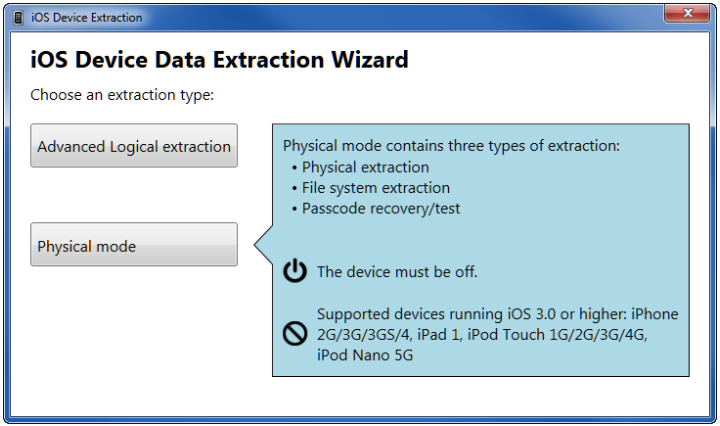
Vous pouvez effectuer une extraction physique et une extraction de systèmes de fichiers des appareils suivants utilisant iOS version 3.0 ou plus récente :

- iPhone 2G
- iPhone 3G
- iPhone 3GS
- iPhone 4
- iPad 1

- iPod Touch 1G
- iPod Touch 2G
- iPod Touch 3G
- iPod Touch 4G
- iPod Nano 5G

10.1.2.1. Effectuer une extraction physique d'appareils iOS non cryptés

1) Sélectionnez **Extraire > Extraction d'appareils iOS** ou cliquez sur pour lancer l'extraction d'appareil iOS.


iOS Device Extraction
iOS Device Data Extraction Wizard
Choose an extraction type:
Advanced Logical extraction
Physical mode
Physical mode contains three types of extraction:
• Physical extraction
• File system extraction
• Passcode recovery/test
The device must be off.
Supported devices running iOS 3.0 or higher: iPhone 2G/3G/3GS/4, iPad 1, iPod Touch 1G/2G/3G/4G, iPod Nano 5G

2) Cliquez sur **Mode physique**.

   Lors de la première exécution d'iOS Device Extraction, ou lorsqu'un nouveau pack correctif est disponible, vous êtes invité à télécharger le pack correctif de l'appareil iOS. Le pack correctif contient les fonctions les plus récentes qui permettent à iOS Device Extraction de fonctionner avec de nombreux appareils et versions iOS. Selon la qualité de votre connexion Internet, le téléchargement peut être assez long.

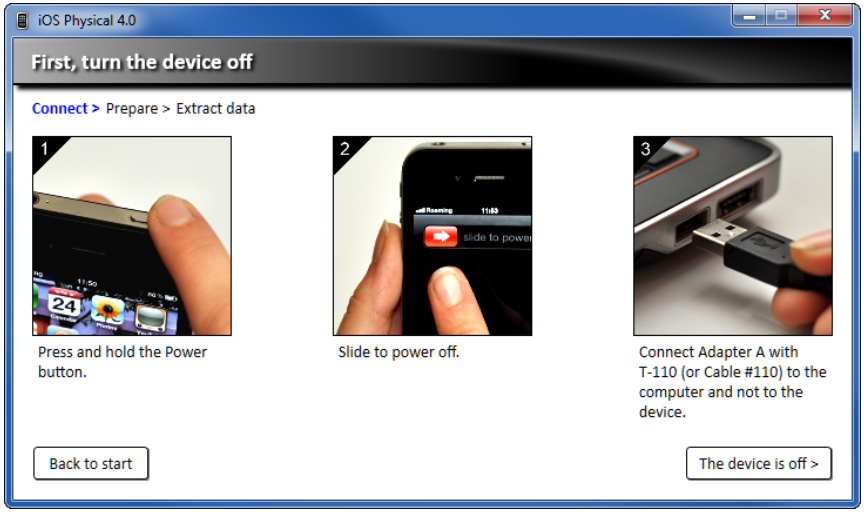
   Si votre ordinateur n'est pas connecté à Internet, utilisez un ordinateur connecté pour télécharger le pack correctif le plus récent, de la façon suivante :

   a) Rendez-vous sur la page **http://www.cellebrite.com/ios**.

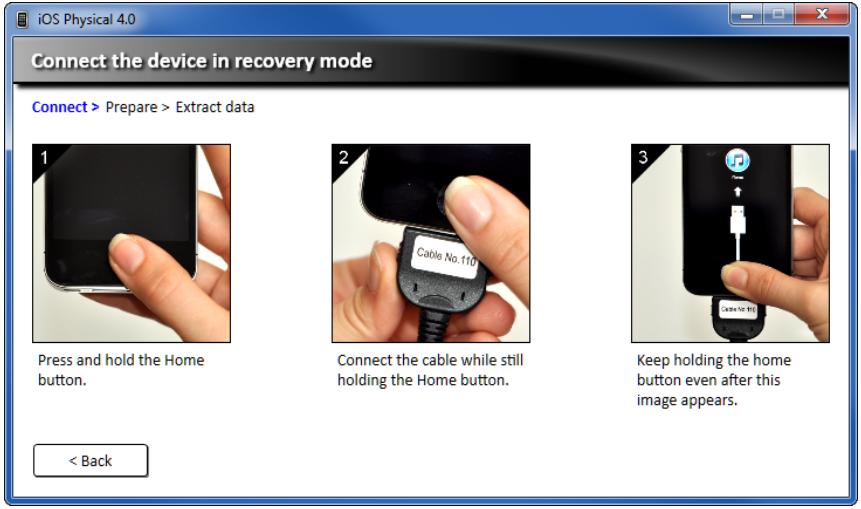
   b) Cliquez sur **Télécharger** et enregistrez et copiez le fichier sur l'ordinateur qui utilise iOS Device Extraction.

   c) Lorsque vous êtes invité à installer le pack correctif, cliquez sur **Installer à partir du fichier**, puis accédez à l'emplacement du fichier du pack correctif et cliquez sur **OK**.

3) Suivez les instructions qui s'affichent pour éteindre l'appareil iOS, puis cliquez sur **L'appareil est éteint**.


iOS Physical 4.0
First, turn the device off
Connect > Prepare > Extract data
1
Press and hold the Power button.
2
Slide to power off.
3
Connect Adapter A with T-110 (or Cable #110) to the computer and not to the device.
Back to start
The device is off >

4) Suivez les instructions qui s'affichent pour activer l'appareil iOS, puis cliquez sur **Mode récupération**.


iOS Physical 4.0
Connect the device in recovery mode
Connect > Prepare > Extract data
1
Press and hold the Home button.
2
Cable No.110
Connect the cable while still holding the Home button.
3
Keep holding the home button even after this image appears.
< Back

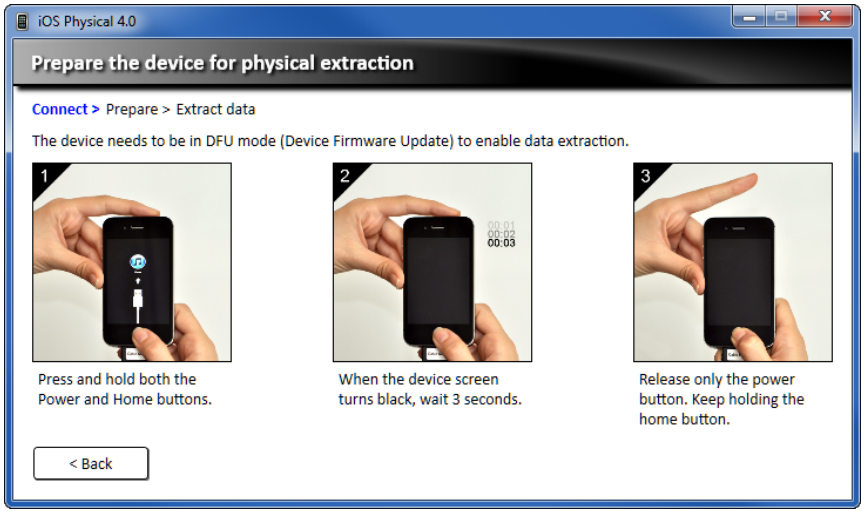
Le processus passe automatiquement à l'étape suivante.

Après détection d'un appareil en **Mode récupération**, iOS Device Extraction affiche des informations sur l'appareil, telles que le numéro de série, la version matérielle, la version iOS, etc.

5) Si vous avez besoin de ces informations, cliquez sur **Copier** les copier sur le presse-papier.

REMARQUE : Lorsque plusieurs versions sont affichées, la version de l'appareil peut être n'importe laquelle. Par exemple, si la version indique **4.0-4.0.2**, la version réelle peut être 4.0, 4.0.1 ou 4.0.2.

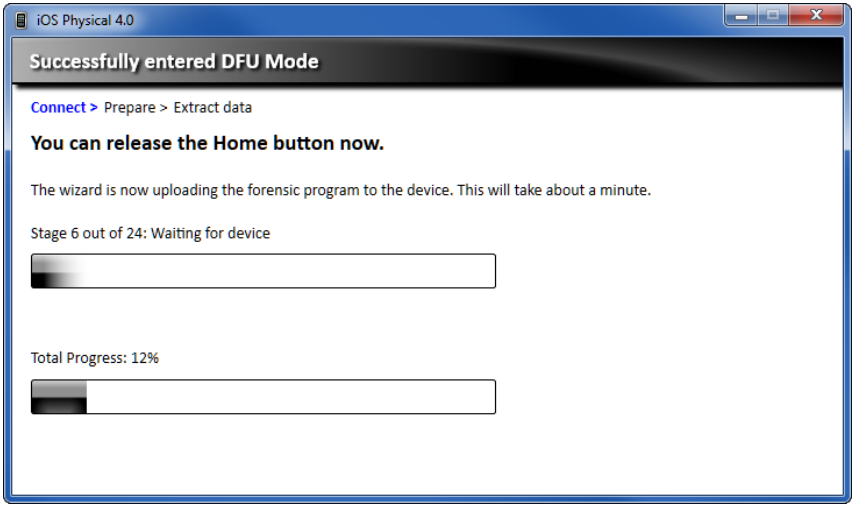
6) Cliquez sur **Suivant** pour continuer.
7) Suivez les instructions qui s'affichent pour configurer l'appareil en mode DFU (mise à niveau des micrologiciels de l'appareil).


iOS Physical 4.0
Prepare the device for physical extraction
Connect > Prepare > Extract data
The device needs to be in DFU mode (Device Firmware Update) to enable data extraction.
1
Press and hold both the Power and Home buttons.
2
00:01
00:02
00:03
When the device screen turns black, wait 3 seconds.
3
Release only the power button. Keep holding the home button.
< Back

iOS Device Extraction n'affecte pas les micrologiciels ou les données utilisateur de l'appareil.

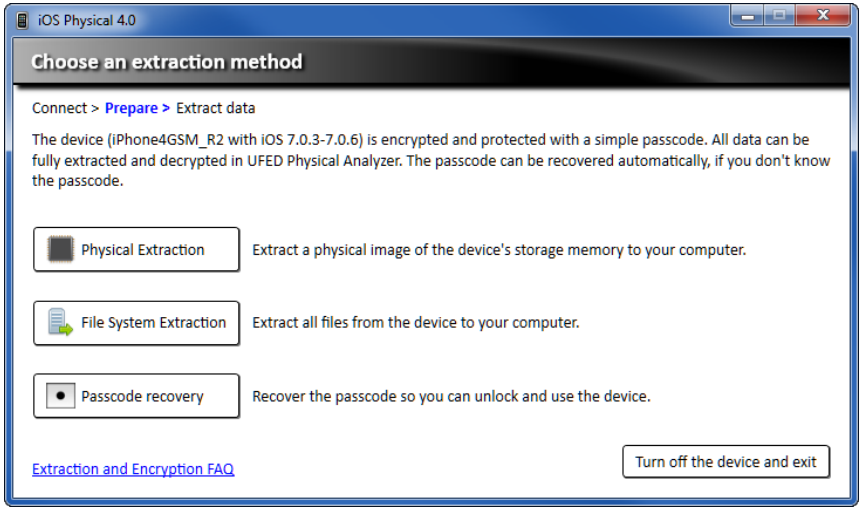
REMARQUE : Cette étape soit être respectée de façon précise. Si l'appareil est accidentellement allumé, débranchez le câble, éteignez l'appareil, puis revenez à l'étape 4.

Lorsque l'appareil est en mode DFU, un programme d'investigation requis pour l'extraction est importé automatiquement sur celui-ci.


iOS Physical 4.0
Successfully entered DFU Mode
Connect > Prepare > Extract data
You can release the Home button now.
The wizard is now uploading the forensic program to the device. This will take about a minute.
Stage 6 out of 24: Waiting for device
Total Progress: 12%

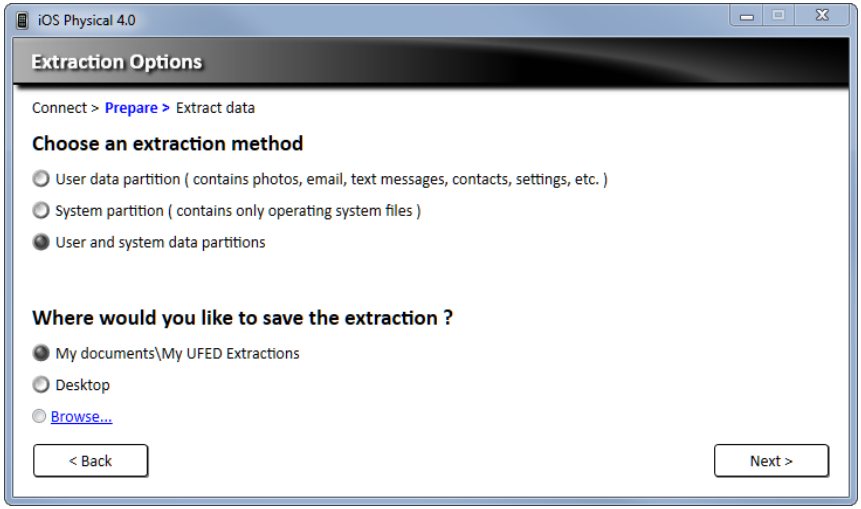
L'appareil est maintenant prêt pour l'extraction.

8) Choisissez le type d'extraction souhaité.


iOS Physical 4.0
Choose an extraction method
Connect > Prepare > Extract data
The device (iPhone4GSM_R2 with iOS 7.0.3-7.0.6) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.
Physical Extraction
Extract a physical image of the device's storage memory to your computer.
File System Extraction
Extract all files from the device to your computer.
Passcode recovery
Recover the passcode so you can unlock and use the device.
Extraction and Encryption FAQ
Turn off the device and exit

9) Choisissez la méthode d'extraction souhaitée :
    - Pour l'extraction physique : **Partition de données utilisateur**, **Partition du système** ou **les deux**.
    - Pour l'extraction d'un système de fichiers : **Partition de données utilisateur** ou **les deux**.

Choisissez l'**emplacement** où vous souhaitez enregistrer les données extraites. Vous pouvez les enregistrer localement sur l'ordinateur ou sur un dispositif de stockage amovible.


iOS Physical 4.0
Extraction Options
Connect > Prepare > Extract data
Choose an extraction method
User data partition (contains photos, email, text messages, contacts, settings, etc.)
System partition (contains only operating system files)
User and system data partitions
Where would you like to save the extraction ?
My documents\My UFED Extractions
Desktop
Browse...
< Back
Next >

10) Cliquez sur **Suivant** pour continuer.

REMARQUE : Si l'appareil est verrouillé par un mot de passe, consultez la section ***Effectuer une extraction physique d'appareils cryptés*** (page ***210***).

11) Attendez la fin du processus d'extraction.

Sa durée varie en fonction de la méthode d'extraction, du modèle de l'appareil, de la quantité de données sur l'appareil, de l'ordinateur qui effectue l'extraction et d'autres paramètres.

Les options suivantes sont proposées à la fin du processus d'extraction :

- **Ouvrir dans UFED Physical Analyzer** – charge le fichier d'extraction dans UFED Physical Analyzer.
- **Ouvrir l'emplacement du fichier** – ouvre le dossier qui contient les fichiers d'extraction.
- **Éteindre l'appareil et quitter** – éteint l'appareil et le remet en mode normal.
- **Retour aux options d'extraction** – revient à l'écran des méthodes d'extraction (étape 8).

12) Éteint l'appareil et le remet en mode normal.

10.1.2.2. Effectuer une extraction physique d'appareils cryptés

iOS Device Extraction peut extraire les données d'appareils cryptés. La quantité de données pouvant être extraites dépend du type de mot de passe protégeant l'appareil.

Il existe deux types de mots de passe :

- Mot de passe simple : 4 chiffres entre 0 et 9 (par ex. 1234, 8787, 2580, etc.)
- Mot de passe complexe : n'importe quelle combinaison de chiffres, lettres et symboles (par ex. 93qP@Mv, iLoVeYoU, etc.)

Le processus de décryptage a lieu dans UFED Physical Analyzer, et non pas pendant l'extraction physique d'appareil iOS. La plupart des données, telles que les contacts, messages, photos, certains e-mails, etc. peuvent être décryptées sans connaître le mot de passe. Cependant, pour décrypter certains mots de passe et e-mails enregistrés, vous devez connaître le mot de passe de l'appareil.

Si l'appareil est verrouillé par un mot de passe simple, iOS Device Extraction récupère automatiquement ce mot de passe pour vous. Si l'appareil est verrouillé par un mot de passe complexe, vous pouvez essayer autant de mots de passe que vous le souhaitez, ou poursuivre l'extraction sans pouvoir décrypter certains mots de passe et e-mails enregistrés.

Si l'appareil n'est pas verrouillé par un mot de passe, toutes les données peuvent être extraites, même si l'appareil est crypté.

10.1.2.2.1. Extraction de données d'un appareil avec mot de passe simple

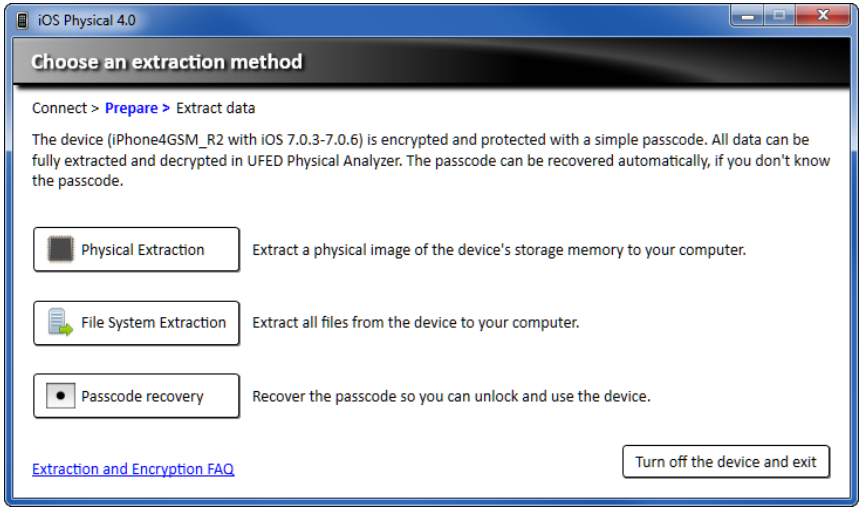
1) Suivez les étapes 1 à 7 de la section ***Effectuer une extraction physique d'appareils iOS non cryptés*** (page ***201***).

   Lorsque l'appareil est prêt pour l'extraction (étape 8), une option **Récupération du mot de passe** supplémentaire est ajoutée aux deux options d'extraction (**Extraction physique** et **Extraction de système de fichiers**).

   L'option de récupération du mot de passe fournit le mot de passe de l'appareil afin de vous permettre de le déverrouiller et de l'utiliser.

2) Pour extraire et récupérer le mot de passe en un seul processus, choisissez **Extraction physique** ou **Extraction de système de fichiers**.

   Les étapes suivantes décrivent un processus d'extraction physique (à partir de l'étape 8 de la section Effectuer une extraction de données), mais elles sont les mêmes pour l'extraction d'un système de fichiers.


iOS Physical 4.0
Choose an extraction method
Connect > Prepare > Extract data
The device (iPhone4GSM_R2 with iOS 7.0.3-7.0.6) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.
Physical Extraction
Extract a physical image of the device's storage memory to your computer.
File System Extraction
Extract all files from the device to your computer.
Passcode recovery
Recover the passcode so you can unlock and use the device.
Extraction and Encryption FAQ
Turn off the device and exit

3) Cliquez sur **Extraction physique**.

4) Choisissez la partition que vous souhaitez extraire et l'emplacement où vous souhaitez enregistrer l'extraction, puis cliquez sur **Suivant**.
5) Si vous ne connaissez pas le mot de passe, cliquez sur **Récupérer le mot de passe pour moi** pour récupérer le mot de passe avant l'extraction.
6) Si vous connaissez le mot de passe, saisissez-le dans le champ de texte ci-dessous. Une coche confirme que le mot de passe saisi est correct.
7) Cliquez sur **Continuer**.

   Le processus d'extraction commence.

10.1.2.2.2. Extraction de données d'un appareil avec mot de passe complexe

1) Suivez les étapes 1 à 7 de la section ***Effectuer une extraction physique d'appareils iOS non cryptés*** (page ***201***).

   Lorsque l'appareil est prêt pour l'extraction (étape 8), une option **Récupération du mot de passe** supplémentaire est ajoutée aux deux options d'extraction (Extraction physique et Extraction de système de fichiers).

   Utilisez l'option **Tester des mots de passe** pour tester et vérifier autant de mots de passe que vous le souhaitez en temps réel. Il est impossible pour iOS Device Extraction de récupérer un mot de passe complexe.

UFED Physical Analyzer décrypte la plupart des données. Cependant, certains mots de passe et fichiers d'e-mails enregistrés ne peuvent pas être décryptés sans connaître le mot de passe complexe.

Les étapes suivantes décrivent une extraction physique (à partir de l'étape 8 de la section Effectuer une extraction de données), mais elles sont les mêmes pour l'extraction d'un système de fichiers.

2) Cliquez sur **Extraction physique**.
3) Choisissez la partition que vous souhaitez extraire et l'emplacement où vous souhaitez enregistrer l'extraction, puis cliquez sur **Suivant**.

iOS Physical 4.0
The passcode is required for the decryption.
Connect > Prepare > Extract data
Use this option if you don't know the passcode:
Recover the passcode for me >
If you know the passcode, enter it here to save time:
The passcode consist of four digits from 0 to 9.
< Back

4) Utilisez une des méthodes suivantes :

- Si vous connaissez le mot de passe complexe, saisissez-le manuellement. Si vous ne connaissez pas le code passe complexe, sachez que certaines données ne seront pas décryptées par UFED Physical Analyzer.
- Utilisez le champ de texte pour tester autant de mots de passe que vous le souhaitez sans bloquer l'appareil. Une coche apparaît lorsque le mot de passe saisi est correct.

5) Utilisez une des méthodes suivantes :
    - Pour commencer l'extraction avec le mot de passe complexe, cliquez sur **Continuer >**.
    - Pour commencer l'extraction sans le mot de passe complexe, cliquez sur **Continuer sans mot de passe**.

   Le processus d'extraction commence.

10.1.3. Effectuer une extraction numérique avancée

Effectuez une extraction numérique avancée depuis UFED Physical Analyzer pour extraire davantage d'informations qu'avec l'extraction numérique à l'aide de l'unité UFED.

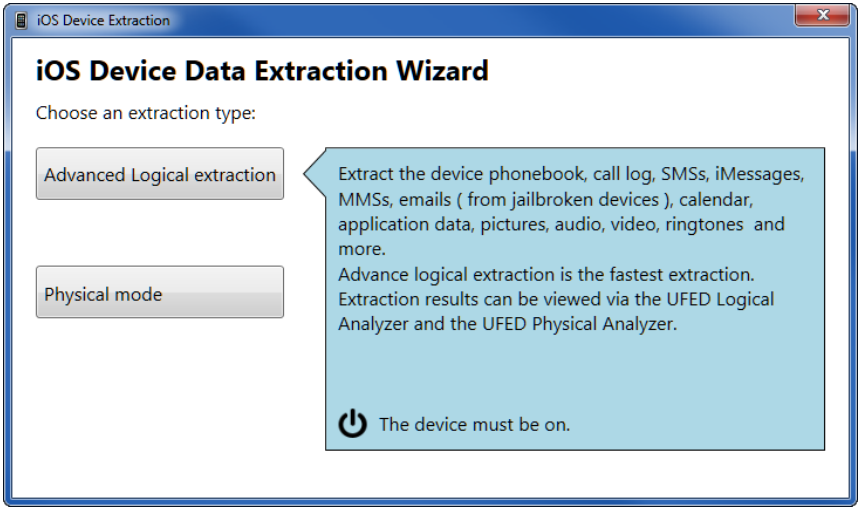
Vous pouvez effectuer une extraction numérique avancée depuis les appareils suivants :

- iPhone 2G/3G/3GS/4/4s/5/5s/5c
- iPad 1/2/3/4/mini
- iPod Touch 1G/2G/3G/4G
- iPod Nano 5G

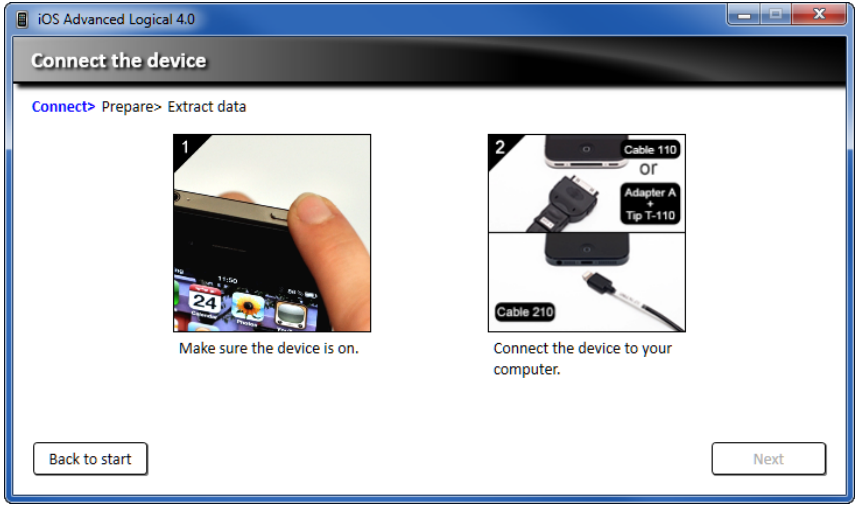
10.1.3.1. Effectuer une extraction numérique avancée

1) Sélectionnez **Extraire > Extraction d'appareils iOS** ou cliquez sur pour lancer l'extraction d'appareil iOS.

2) Cliquez sur **Extraction numérique avancée**.


iOS Device Extraction
iOS Device Data Extraction Wizard
Choose an extraction type:
Advanced Logical extraction
Physical mode
Extract the device phonebook, call log, SMSs, iMessages, MMSs, emails (from jailbroken devices), calendar, application data, pictures, audio, video, ringtones and more.
Advance logical extraction is the fastest extraction. Extraction results can be viewed via the UFED Logical Analyzer and the UFED Physical Analyzer.
The device must be on.

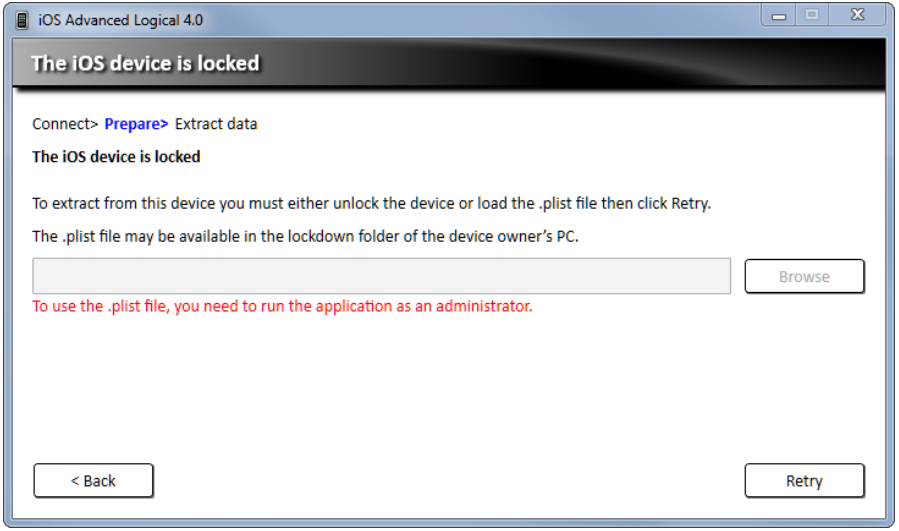
3) Suivez les instructions qui s'affichent pour allumer l'appareil iOS et le connecter à votre ordinateur, puis cliquez sur **Suivant**.



REMARQUE : Si l'appareil connecté n'est pas reconnu, déconnectez-le, puis reconnectez-le à un port USB à l'arrière de l'ordinateur.

Si l'appareil iOS est verrouillé, l'écran **Appareil verrouillé** s'affiche. Si le fichier .plist pour l'appareil verrouillé est disponible sur le PC du propriétaire de l'appareil, alors ce fichier .plist peut être chargé sur l'écran **Appareil verrouillé**. Cliquez ensuite sur **Réessayer**. Si l'appareil est verrouillé et qu'aucun fichier .plist n'est disponible, cliquez sur **Fermer**.

REMARQUE : Pour utiliser le fichier .plist, vous devez exécuter l'application UFED en tant qu'administrateur.


iOS Advanced Logical 4.0
The iOS device is locked
Connect> Prepare> Extract data
The iOS device is locked
To extract from this device you must either unlock the device or load the .plist file then click Retry.
The .plist file may be available in the lockdown folder of the device owner's PC.
Browse
To use the .plist file, you need to run the application as an administrator.
< Back
Retry

4) Choisissez une **Méthode** d'extraction numérique avancée. Selon que l'appareil est **bloqué** et/ou **crypté** ou non, différentes méthodes d'extraction sont disponibles :

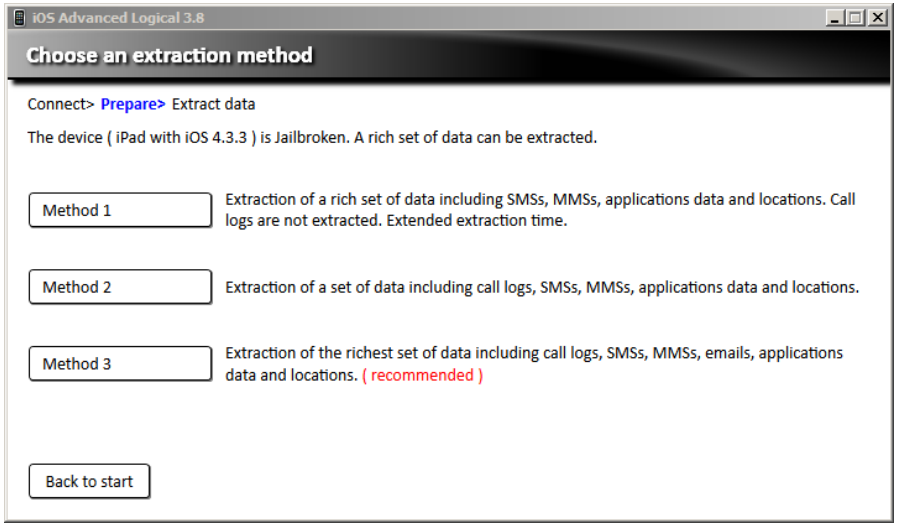
   a) Méthode 1 – Extraction d'un ensemble de données important comprenant les SMS, MMS, données d'application et emplacements. Journaux des appels, corps des e-mails et pièces jointes ne sont pas extraits. Durée d'extraction prolongée.

   b) Méthode 2 – Extraction d'un ensemble de données comprenant les journaux d'appels, SMS, MMS, données d'application et emplacements. Cette procédure de décodage peut nécessiter la saisie du mot de passe de sauvegarde iTunes.

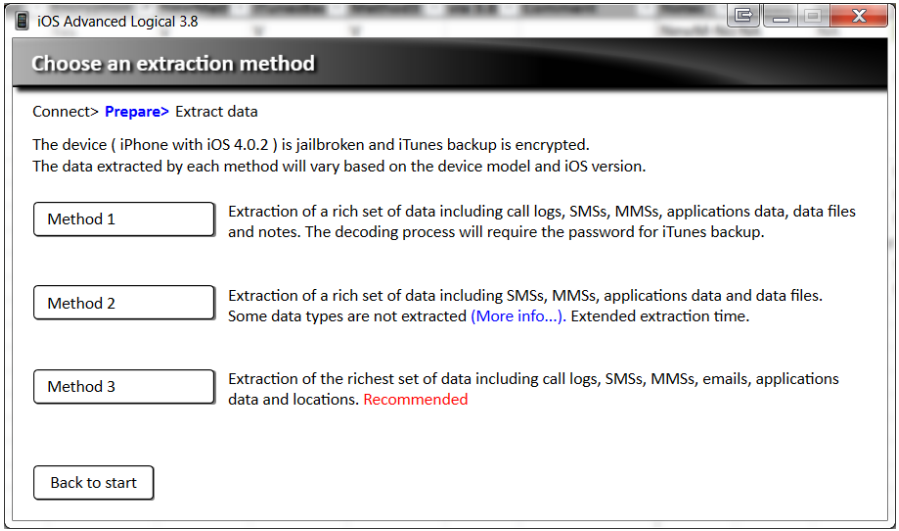
   c) Méthode 3 – Extraction de l'ensemble de données le plus complet comprenant les journaux d'appels, SMS, MMS, e-mails, données d'application et emplacements.

En outre, l'application indique une méthode recommandée spécifique en fonction de la configuration de la sauvegarde iTunes et de si l'appareil est bloqué ou non.

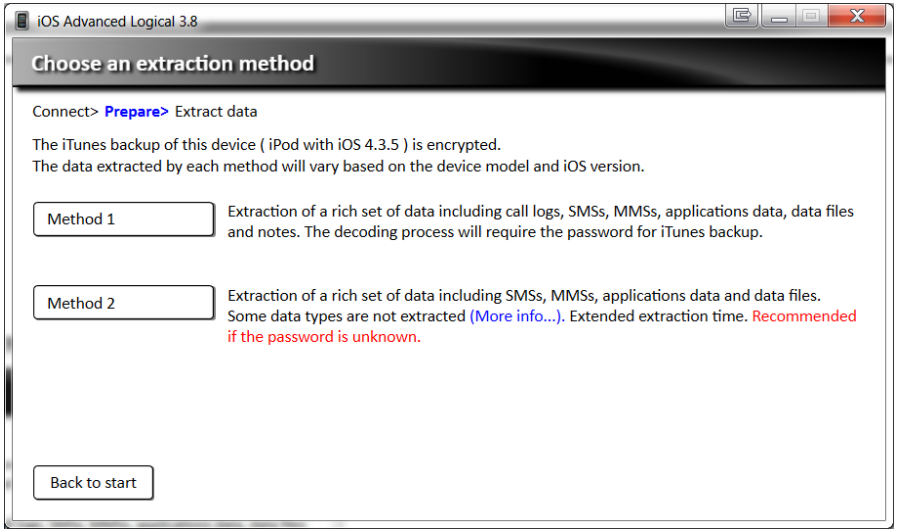
Pour un appareil iOS **débloqué**, l'écran suivant s'affiche :


iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The device (iPad with iOS 4.3.3) is Jailbroken. A rich set of data can be extracted.
Method 1
Extraction of a rich set of data including SMSs, MMSs, applications data and locations. Call logs are not extracted. Extended extraction time.
Method 2
Extraction of a set of data including call logs, SMSs, MMSs, applications data and locations.
Method 3
Extraction of the richest set of data including call logs, SMSs, MMSs, emails, applications data and locations. (recommended)
Back to start

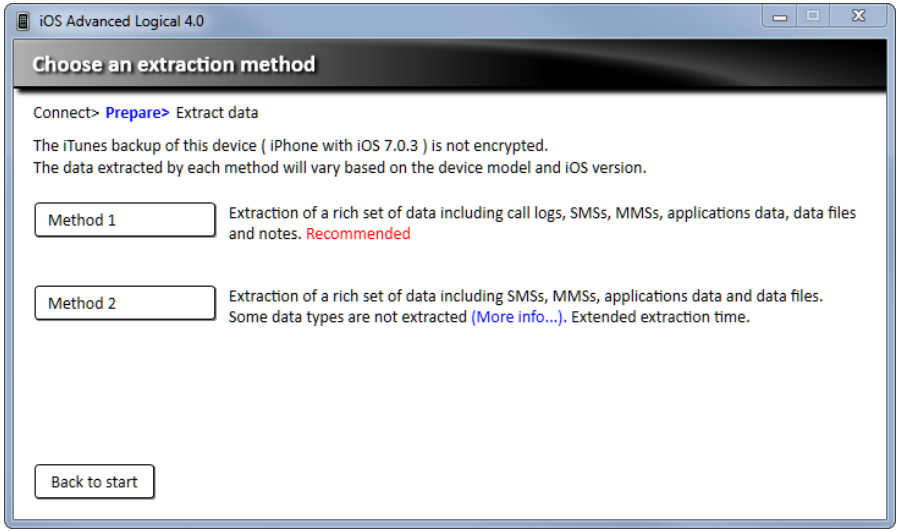
Pour un appareil iOS **débloqué et crypté**, l'écran suivant s'affiche :


iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The device (iPhone with iOS 4.0.2) is jailbroken and iTunes backup is encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup.
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time.
Method 3
Extraction of the richest set of data including call logs, SMSs, MMSs, emails, applications data and locations. Recommended
Back to start

Pour un appareil iOS **bloqué et crypté**, l'écran suivant s'affiche :

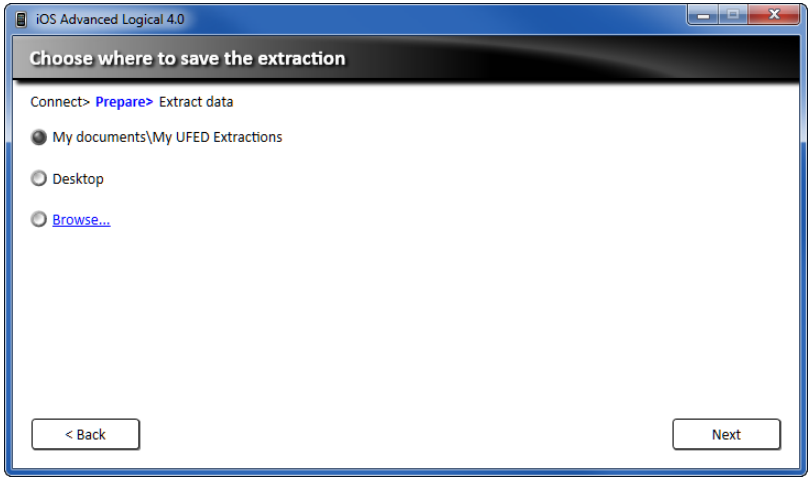

iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The iTunes backup of this device (iPod with iOS 4.3.5) is encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup.
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time. Recommended if the password is unknown.
Back to start

Pour un appareil iOS **bloqué et non crypté**, l'écran suivant s'affiche :


iOS Advanced Logical 4.0
Choose an extraction method
Connect> Prepare> Extract data
The iTunes backup of this device (iPhone with iOS 7.0.3) is not encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. Recommended
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time.
Back to start

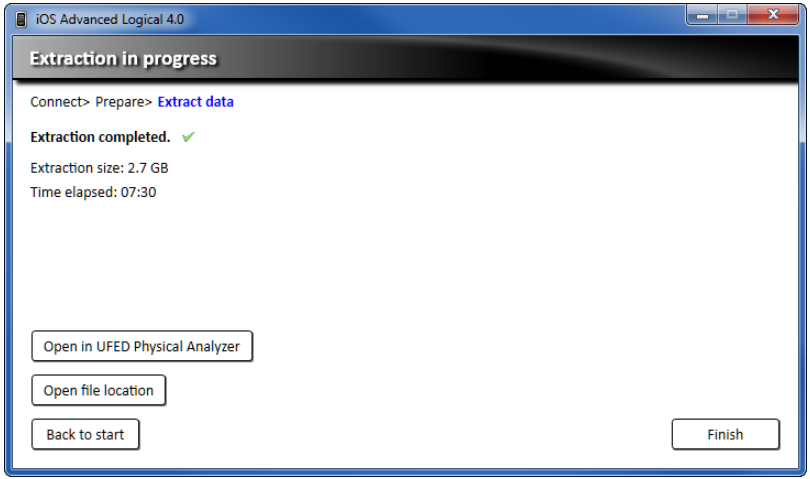
REMARQUE : La durée de l'extraction dépend de la quantité de données présente sur l'appareil iOS et de la méthode choisie. Une extraction avec la **Méthode 2** effectuée sur un appareil beaucoup utilisé peut durer plusieurs HEURES.

5) Choisissez l'emplacement où vous souhaitez enregistrer les données extraites. Assurez-vous que l'espace disque disponible est suffisant à l'emplacement choisi. Vous pouvez enregistrer les données localement sur l'ordinateur, sur un dispositif de stockage amovible ou sur le réseau.



6) Cliquez sur **Suivant** pour continuer.

7) Une barre de progression s'affiche. Attendez la fin du processus d'extraction.



REMARQUE : Sa durée varie en fonction de la méthode d'extraction, du modèle de l'appareil, de la quantité de données sur l'appareil, de l'ordinateur qui effectue l'extraction et d'autres paramètres.

L'extraction numérique avancée est enregistrée à l'emplacement choisi, sous la forme d'un fichier *.UFD et d'un fichier *.TAR.

Ouvrez l'extraction numérique avancée dans UFED Physical Analyzer pour accéder à toutes les informations extraites, y compris les informations effacées.

REMARQUE : Vous ne pouvez pas accéder aux informations supprimées extraites si vous ouvrez l'extraction dans UFED Logical Analyzer.

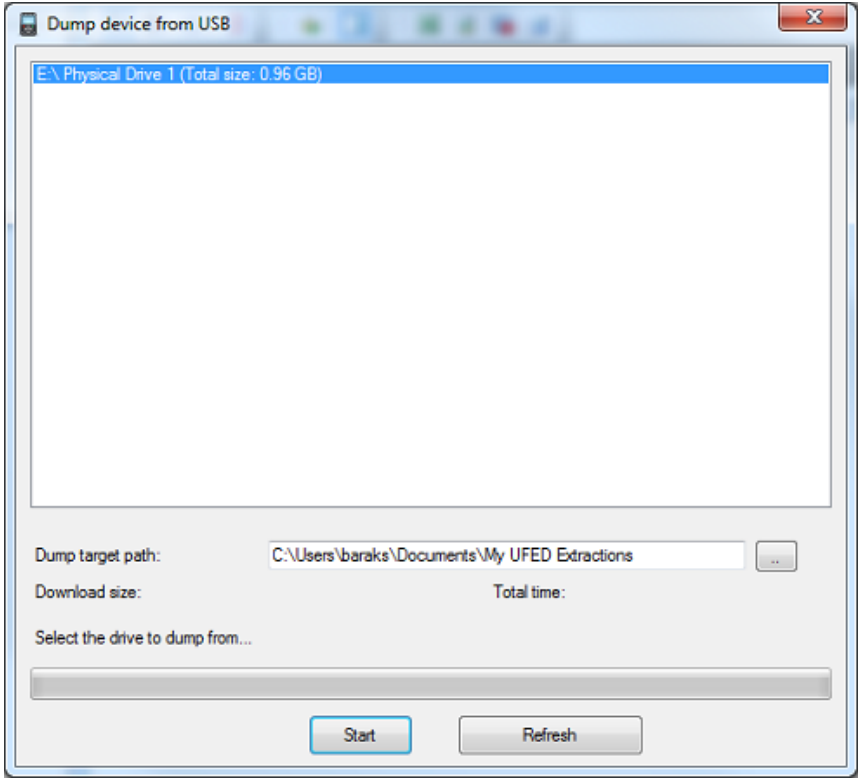
8) Choisissez l'une des options suivantes :
   - **Ouvrir dans UFED Physical Analyzer** – charge le fichier d'extraction dans UFED Physical Analyzer.
   - **Ouvrir l'emplacement du fichier** – ouvre le dossier qui contient les fichiers d'extraction.
   - **Revenir au début** – revient à l'écran des méthodes d'extraction.
   - **Terminer** – ferme l'extraction d'appareil iOS.

10.2. Extraction du GPS ou des appareils de stockage de masse

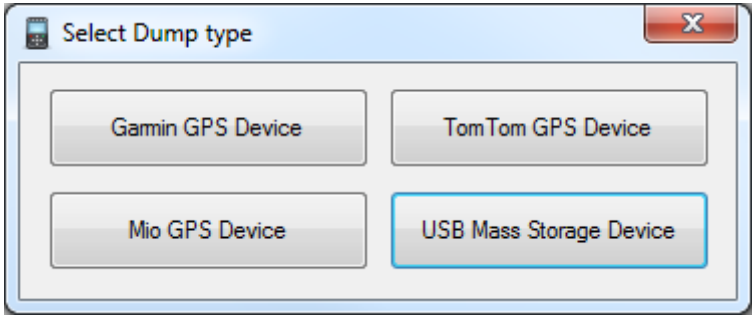
Extraire et enregistrer des données depuis un GPS (Garmin, Mio et TomTom) ou un appareil de stockage de masse

REMARQUE : Seuls les utilisateurs administrateurs peuvent lire les données d'appareils GPS. Si vous n'êtes pas un administrateur, fermez UFED Physical Analyzer, cliquez avec le bouton droit de la souris sur l'icône UFED Physical Analyzer sur votre bureau, et sélectionnez **Exécuter en tant qu'administrateur**.

1) Connectez le GPS ou l'appareil de stockage de masse à votre PC.
2) Sélectionnez **Extraire** > **Extraire GPS/Appareil de stockage de masse** ou cliquez sur .

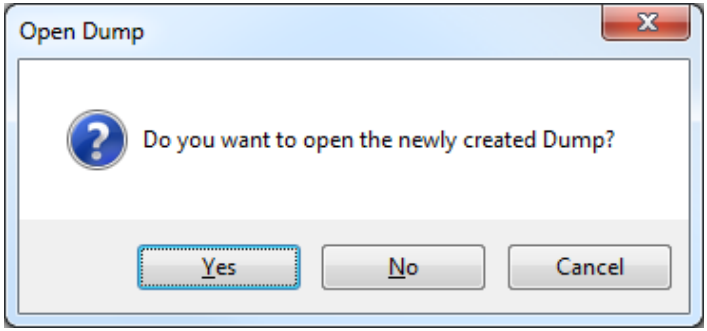

Dump device from USB
E:\ Physical Drive 1 (Total size: 0.96 GB)
Dump target path:
C:\Users\baraks\Documents\My UFED Extractions
...
Download size:
Total time:
Select the drive to dump from...
Start
Refresh

3) Sélectionnez l'appareil.
4) Utilisez une des méthodes suivantes :
    - Saisissez le chemin de l'emplacement où vous souhaitez enregistrer les données extraites de l'appareil.
    - Cliquez sur et sélectionnez l'emplacement souhaité.
5) Cliquez sur **Démarrer**.



6) Sélectionnez le type.

L'extraction commence. Lorsqu'elle est terminée, le message suivant s'affiche :



7) Cliquez sur **Oui** pour ouvrir l'extraction.

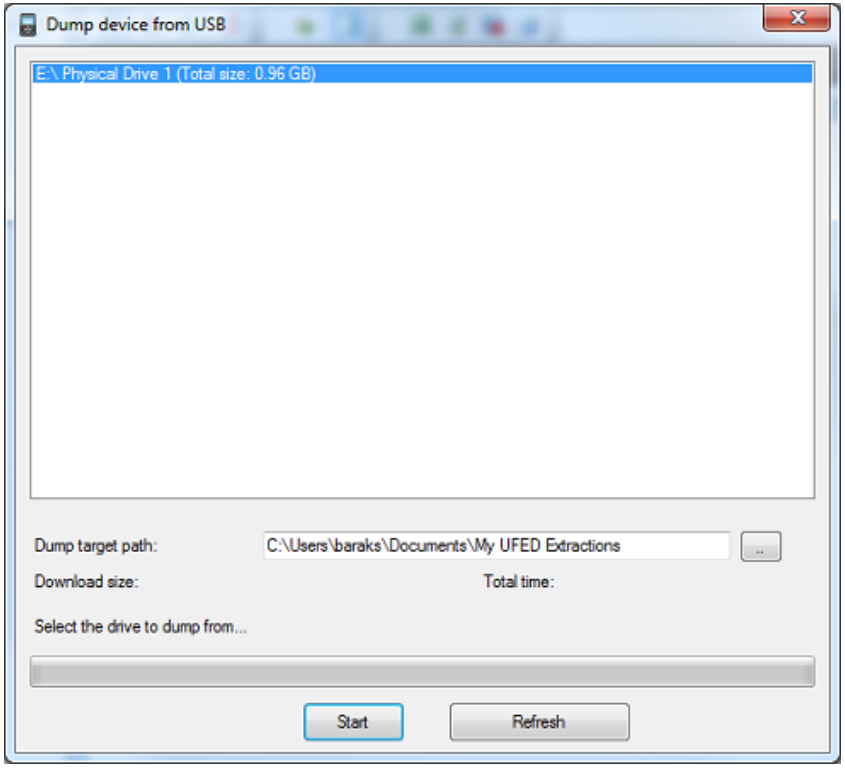
10.2.1. Lire des données depuis un appareil GPS ou de stockage de masse

Lire et enregistrer des données depuis un appareil GPS (Garmin, Mio et TomTom) ou un appareil de stockage de masse

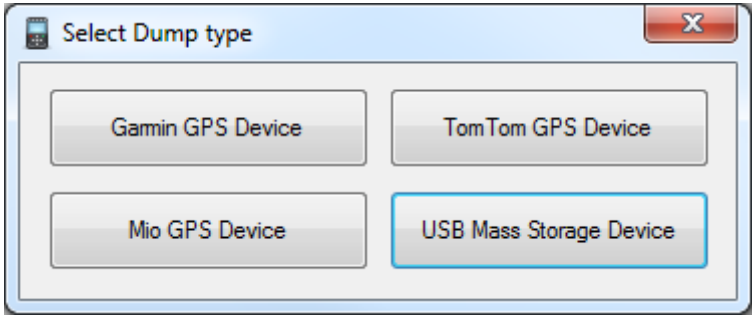
REMARQUE : Seuls les utilisateurs administrateurs peuvent lire les données d'appareils GPS. Si vous n'êtes pas un administrateur, fermez UFED Physical Analyzer, cliquez avec le bouton droit de la souris sur l'icône UFED Physical Analyzer sur votre bureau, et sélectionnez **Exécuter en tant qu'administrateur**.

1) Connectez le GPS ou l'appareil de stockage de masse à votre PC.

2) Sélectionnez **Outils** > **Vidage GPS/Appareil de stockage de masse**, ou cliquez sur .

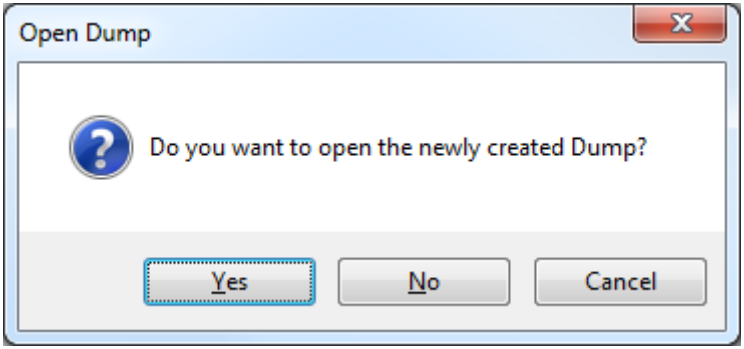


3) Sélectionnez l'appareil.
4) Utilisez une des méthodes suivantes :
    - Saisissez le chemin de l'emplacement où vous souhaitez enregistrer les données extraites de l'appareil.
    - Cliquez sur ... et sélectionnez l'emplacement souhaité.
5) Cliquez sur **Démarrer**.



6) Sélectionnez le type de vidage.

L'extraction commence. Lorsqu'elle est terminée, le message suivant s'affiche :



7) Cliquez sur **Oui** pour ouvrir l'extraction.

Chapitre 11 : **Paramètres avancés**

11.1. Travailler avec TomTom

TomTom génère des fichiers journaux de trajet cryptés par l'appareil, uniquement si les utilisateurs de TomTom choisissent de partager leurs informations de localisation avec TomTom. TomTom consigne la localisation de l'appareil dans les fichiers journaux de trajet. Exportez le fichier XML TomTom généré à partir des journaux de trajet, et envoyez-le à Cellebrite pour qu'il soit traité. Une fois qu'il vous a été renvoyé, vous pouvez afficher la plupart des informations de localisation disponibles sur le fichier à l'aide de UFED Physical Analyzer.

Pour plus d'informations sur l'extraction de données d'un appareil TomTom, consultez la section ***Lire des données depuis un appareil GPS ou de stockage de masse*** (page ***230***).

Pour en savoir plus sur les géolocalisations, consultez la section ***À propos des données de localisation*** (page ***149***).

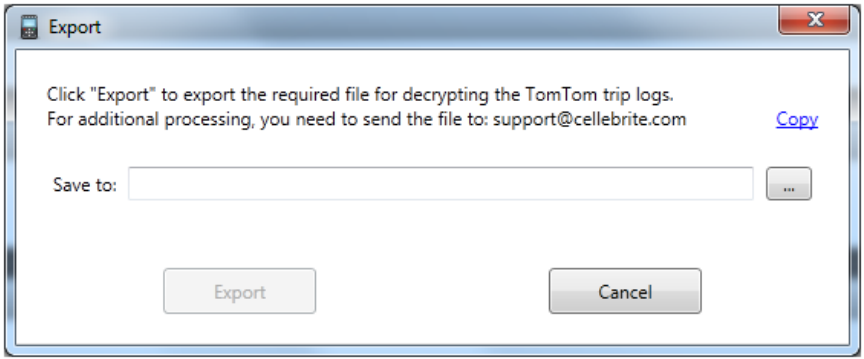
REMARQUE : Il n'est pas possible de récupérer toutes les informations contenues dans le fichier d'extraction TomTom.

REMARQUE : Le service de traitement peut prendre plusieurs jours, selon de volume de données et le nombre de demandes. Ce service est actuellement gratuit, mais est susceptible d'être modifié.

REMARQUE : Vous devez ouvrir l'extraction TomTom dans UFED Physical Analyzer avant d'exporter ou d'importer le fichier XML.

11.1.1. Exporter un fichier TomTom

1) Ouvrez une extraction depuis un appareil TomTom.
2) Dans le menu **Outils**, sélectionnez **TomTom** > **Exporter**.



3) Accédez à l'emplacement où vous souhaitez enregistrer le fichier d'extraction TomTom exporté, puis cliquez sur **Enregistrer**.

   Le fichier d'extraction TomTom est enregistré comme fichier GPS.TomTomExport.xml.

   REMARQUE : Le fichier ne contient pas d'informations personnelles de l'utilisateur telles que la localisation.

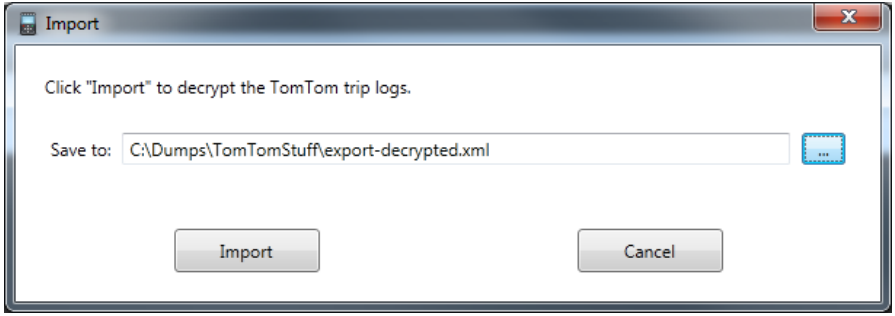
4) Envoyez le fichier GPS.TomTomExport.xml à l'adresse : support@cellebrite.com. Pour les clients aux États-Unis : support@cellebriteusa.com.

   Le fichier GPS.TomTomExport.xml est traité par l'équipe d'assistance de Cellebrite. Votre demande est placée dans une file d'attente dans le service d'assistance de Cellebrite. Le traitement du fichier d'extraction TomTom peut prendre quelques jours.

11.1.2. Importer un fichier TomTom

Une fois que l'assistance Cellebrite vous a renvoyé votre fichier XML TomTom traité, importez-le sur UFED Physical Analyzer.

1) Ouvrez l'extraction TomTom correspondant au fichier *.xml.
2) Dans le menu **Outils**, sélectionnez **TomTom** > **Importer**.



3) Cliquez sur ... et accédez à l'emplacement du fichier d'extraction TomTom *.xml qui vous a été renvoyé, puis cliquez sur **Ouvrir**.
4) Cliquez sur **Importer**.

   Le fichier TomTom *.xml est importé vers UFED Physical Analyzer. L'élément d'arborescence **Localisations** est rempli.
5) Double-cliquez sur **Localisations** pour ouvrir l'élément d'arborescence dans un onglet de données.

   L'onglet montre la localisation de l'appareil toutes les trois secondes avec un horodatage indiquant la date et l'heure, ainsi que ses coordonnées géographiques.

REMARQUE : Il n'est pas possible de récupérer toutes les informations contenues dans le fichier d'extraction TomTom.

11.2. Reconstituer des images

Effectuez une reconstitution d'image pour récupérer des fichiers image JPEG ou des fragments incomplets ou corrompus, ce qui indique qu'ils ont été supprimés par l'utilisateur. La reconstitution d'image récupère et restaure les images dans la mesure du possible.

Pour effectuer une reconstitution d'image, vous devez le demander. Elle n'est pas effectuée lorsque UFED Physical Analyzer ouvre l'extraction physique.

REMARQUE : La reconstitution d'image est disponible uniquement pour les extractions physiques.

La reconstitution d'image est un processus qui peut prendre du temps. Pendant son traitement, vous pouvez continuer de travailler en parallèle dans UFED Physical Analyzer.

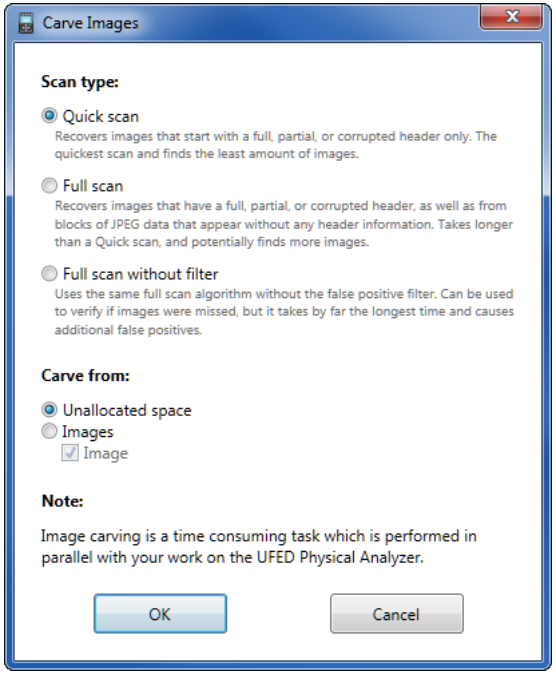
11.2.1. Rechercher les images reconstituées

1) Utilisez une des méthodes suivantes :
    - Cliquez sur .

REMARQUE : Lorsque vous cliquez sur dans la barre d'outils, la recherche s'applique au projet actif, c'est-à-dire le dernier projet sur lequel vous avez cliqué.

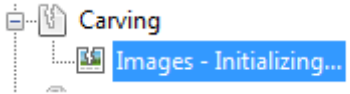
- Si vous n'avez pas recherché d'images reconstituées au cours de la session actuelle, double-cliquez sur l'élément d'arborescence **Reconstitution** > **Images**.
- Si vous avez déjà recherché des images reconstituées au cours de la session actuelle, cliquez avec le bouton droit de la souris sur l'élément d'arborescence **Reconstitution** > **Images**, puis sélectionnez **Rechercher à nouveau**.

L'écran Reconstituer les images s'affiche.


Carve Images
Scan type:
Quick scan
Recovers images that start with a full, partial, or corrupted header only. The quickest scan and finds the least amount of images.
Full scan
Recovers images that have a full, partial, or corrupted header, as well as from blocks of JPEG data that appear without any header information. Takes longer than a Quick scan, and potentially finds more images.
Full scan without filter
Uses the same full scan algorithm without the false positive filter. Can be used to verify if images were missed, but it takes by far the longest time and causes additional false positives.
Carve from:
Unallocated space
Images
Image
Note:
Image carving is a time consuming task which is performed in parallel with your work on the UFED Physical Analyzer.
OK
Cancel

2) Sélectionnez le type de scan :
    - **Scan rapide** : ce scan se déroule en trois étapes, au cours desquelles UFED Physical Analyzer tente de récupérer les images qui commencent uniquement par un en-tête complet, partiel ou corrompu.
    - **Scan complet** : ce scan se déroule en cinq étapes. En plus de récupérer les images qui ont un en-tête complet, partiel ou corrompu, UFED Physical Analyzer tente de récupérer les images dans les blocs de données JPEG qui apparaissent sans en-tête. Un scan complet est plus long qu'un scan rapide, et peut récupérer un plus grand nombre d'images.
    - **Scan complet sans filtre** : ce scan utilise le même algorithme que le scan complet, mais sans le filtre Faux positif. Il peut être utilisé pour vérifier si des images ont été omises, mais dure beaucoup plus longtemps et provoque des faux positifs supplémentaires.
3) Sélectionnez l'emplacement où vous souhaitez rechercher des images pour les reconstituer :
    - **Espace non alloué** : scanne l'espace mémoire non attribué.
    - **Images** : sélectionnez toutes les images que vous souhaitez scanner.
4) Cliquez sur **OK**.

    Le scan commence. Sa progression s'affiche à côté de l'élément d'arborescence **Reconstitution** > **Images**.



11.2.2. Travailler avec les images reconstituées

Ouvrez les onglets d'affichage de données de toutes les images reconstituées, pour les images individuelles, et extrayez les images vers votre ordinateur.

Pour afficher toutes les images trouvées dans l'arborescence de projet :

- Cliquez sur ⊞ pour développer l'élément d'arborescence **Reconstitution** > **Images** .

Pour ouvrir un onglet d'affichage de données pour une image individuelle :

- Double-cliquez sur l'image dans l'arborescence de projet.

  Pour en savoir plus sur le travail avec les images, consultez la section ***Afficher les fichiers image*** (page ***116***).

Pour extraire (vider) les images reconstituées vers votre ordinateur :

1) Cliquez avec le bouton droit de la souris sur l'élément d'arborescence **Reconstitution** > **Images**, puis sélectionnez **Vider**.
2) Dans la fenêtre « Sélectionner dossier », accédez au dossier souhaité, puis cliquez sur **Sélectionner dossier**.

11.3. Vérifier les valeurs de hachage

Une valeur de hachage est une représentation unique et compacte d'un élément de données, qui peut être utilisée pour protéger l'intégrité des données, car il est statistiquement improbable de trouver deux entrées distinctes possédant la même valeur de hachage.

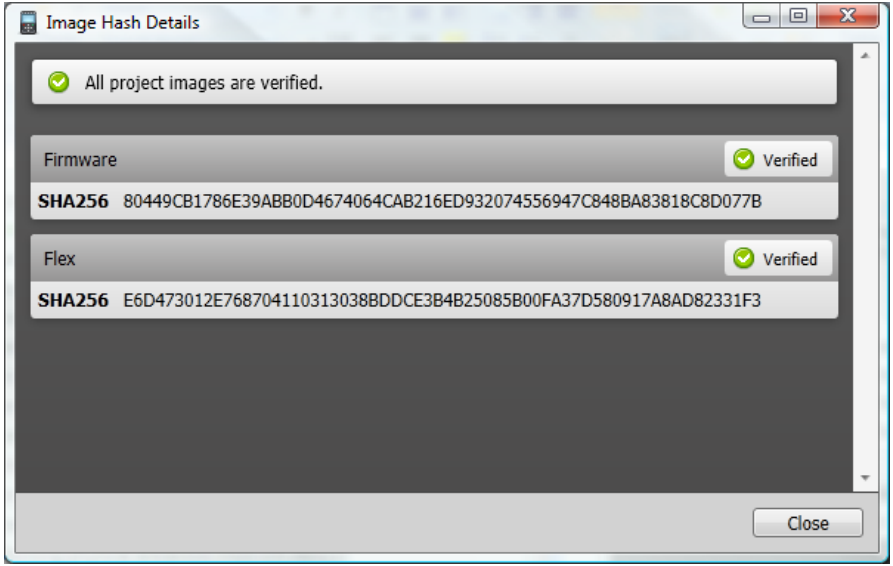
La comparaison des valeurs de hachage de référence, générées au cours du processus d'extraction pour chaque extraction binaire, avec les valeurs de hachage calculées vous permet de vérifier l'intégrité des extractions binaires que vous recevez.

Pour vérifier les valeurs de hachage :

1) Dans l'onglet **Résumé d'extraction** du projet, sélectionnez une des options suivantes :
    - Si les informations de hachage sont disponibles pour le projet, cliquez sur **Vérifier**.
    - Si les informations de hachage ne sont pas disponibles pour le projet, cliquez sur **Calculer les valeurs de hachage**.

    Les informations de hachage sont calculées ou vérifiées. Si aucune donnée de référence n'est disponible, un message **Les valeurs de hachage ont été calculées pour ce projet, mais aucune donnée de référence n'est disponible** s'affiche dans la section **Informations de hachage de l'image** de l'onglet **Résumé d'extraction**.

2) Cliquez sur **Afficher les détails**.



La fenêtre « Détails du hachage de l'image » affiche les résultats de la comparaison entre les valeurs de hachage de référence et calculées pour chaque image.

- Verified indique des valeurs identiques.
- Bad Verification indique que les images ne correspondent pas.

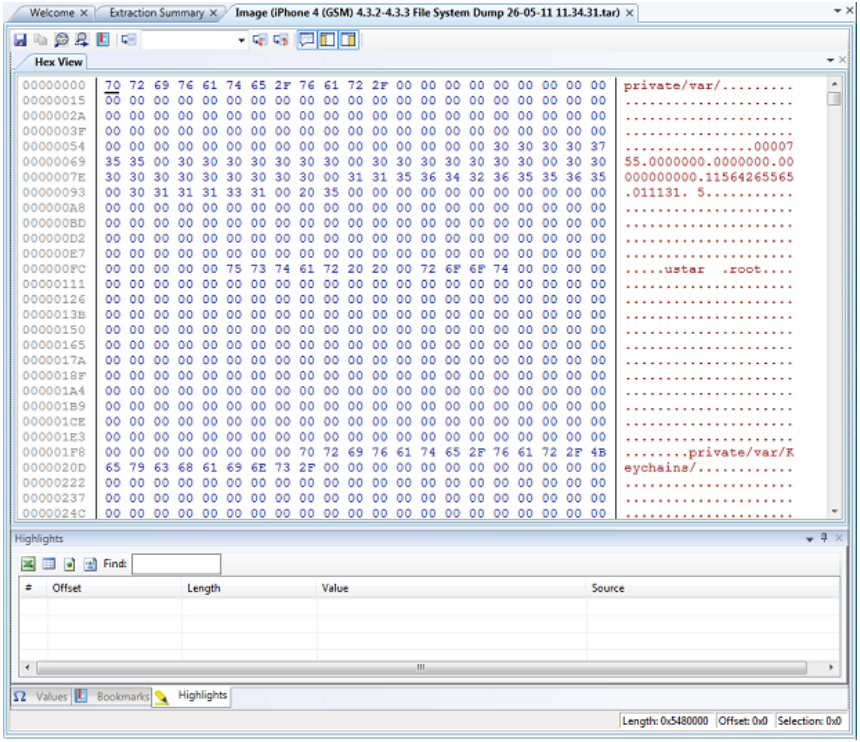
Chapitre 12 : **Travailler avec les données hexadécimales**

L'extraction vous permet d'afficher l'image de l'appareil. Il s'agit d'un ou plusieurs fichiers qui contiennent une copie complète du contenu et de la structure des données sur l'appareil.

Pour accéder à la vue hexadécimale de l'image de l'appareil :

- Dans l'arborescence de projet, développez l'élément **Images** et double-cliquez sur l'image souhaitée.

Un onglet Image s'affiche dans la zone d'affichage des données, montrant une vue hexadécimale des données de l'image.

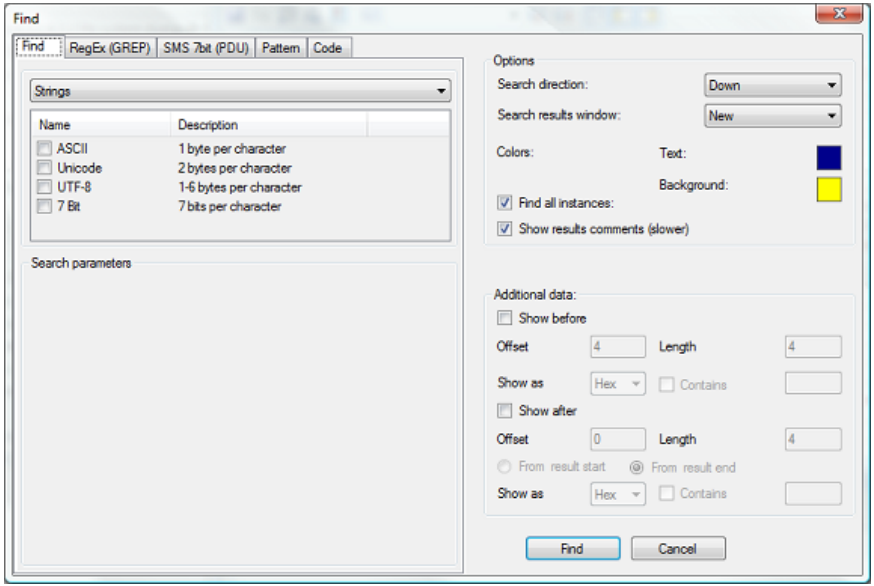


Les onglets d'informations sur l'analyse sont situés sous l'onglet Vue hexadécimale. Ils affichent les types d'informations suivants, en lien direct avec les données hexadécimales affichées :

- **Valeurs** : un grand nombre d'interprétations des valeurs, telles que 8, 16, 32 et 64 bits, divers encodages de chaîne, les formats de date et d'heure, etc., calculés au fur et à mesure pour les données actuelles contenues dans la vue hexadécimale. Consultez la section ***Travailler dans l'onglet Valeurs*** (page ***112***).
- **Signets** : une liste des signets ajoutés aux données hexadécimales affichées. Consultez la section ***Travailler avec les signets*** (page ***304***).
- **Mises en évidence** : une liste des segments de contenu mis en évidence dans les données hexadécimales affichées. Le nombre de résultats mis en évidence apparaît entre parenthèses à côté du nom de l'onglet. Consultez la section ***Travailler dans l'onglet Mises en évidence*** (page ***114***).
- **Rechercher** : affiche les résultats d'une recherche dans les données hexadécimales affichées. Un nouvel onglet Résultats de recherche est ouvert pour chaque recherche effectuée. Le nombre de résultats pour chaque recherche apparaît entre parenthèses à côté du nom de l'onglet.

Pour en savoir plus sur l'onglet Image, consultez la section ***Vue hexadécimale*** (page ***108***).

12.1. Rechercher des informations dans les données hexadécimales et dans les données décodées



La fenêtre « Rechercher » se compose de plusieurs onglets qui vous permettent de rechercher les données hexadécimales dans les modes suivants :

- **Rechercher** – recherche de paramètres spécifiques, tels que des chaînes, des octets, des dates, etc.
- **RegEx (GREP)** – recherche de chaînes utilisant des expressions régulières.
- **SMS 7 bits (PDU)** – recherche de chaînes de texte de SMS.
- **Schéma** – recherche de schémas de texte, dans les cas où le schéma du texte est compris, mais pas le texte lui-même (principalement utilisée pour la recherche en 7 bits pour localiser les SMS).
- **Code** – recherche spécialisée de codes et mots de passe.

REMARQUE : Les modes de **Recherche** ont été conçus avec l'architecture de plug-ins. Les options de recherche peuvent être améliorées et développées en ajoutant de nouveaux plug-ins de recherche.

Pour en savoir plus sur les recherches ciblées, consultez les sections suivantes :

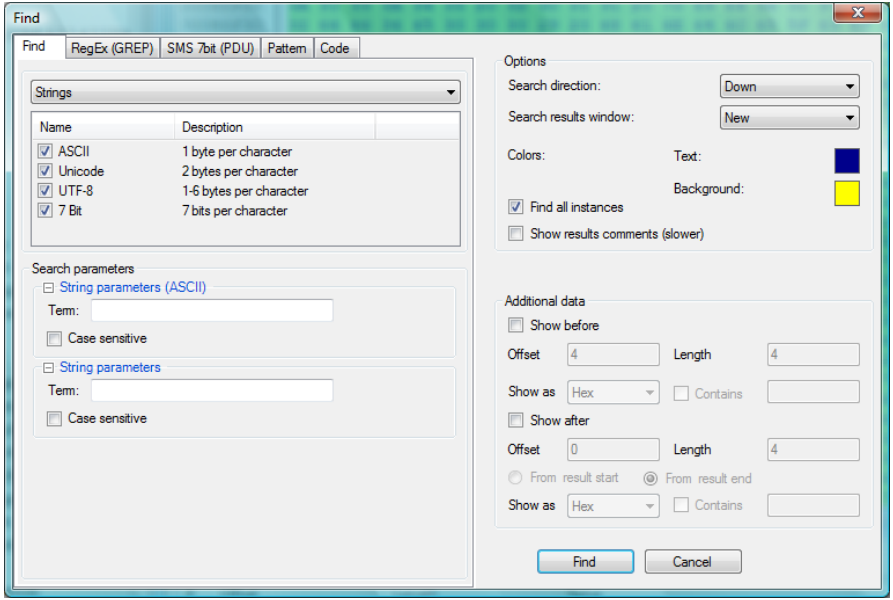
- ***Rechercher des chaînes*** (page ***252***)
- ***Rechercher des octets*** (page ***257***)
- ***Rechercher des dates*** (page ***262***)
- ***Rechercher des numéros SIM ICCID*** (page ***268***)
- ***Rechercher des numéros SMS*** (page ***273***)

- ***Rechercher des expressions régulières (GREP)*** (page ***279***)
- ***Rechercher des chaînes de texte de SMS*** (page ***285***)
- ***Rechercher des schémas*** (page ***291***)
- ***Rechercher des codes et des mots de passe*** (page ***297***)

12.1.1. Rechercher des chaînes

Recherchez des chaînes pour localiser différents types de données dans les données hexadécimales, par exemple messages textuels, numéros de téléphone, noms et toutes autres données de chaîne.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Dans l'onglet **Rechercher**, sélectionnez **Chaînes** dans la liste de types de données.



3) Sélectionnez le type d'encodage du texte à rechercher pour la chaîne donnée :
    - **ASCII**
    - **UNICODE** (principalement pour les caractères non latins)
    - **UTF-8**
    - **7 bits** (principalement pour le texte des SMS)

L'écran **Paramètres de recherche** s'affiche :

4) Sur la page **Paramètres de recherche** :
   a) Dans le champ **Terme** de la zone **Paramètres de la chaîne**, saisissez la chaîne de recherche.
   b) Sélectionnez l'option **Respecter la casse** si nécessaire.
5) Dans la zone **Options** , choisissez les options de recherche souhaitées :
   a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.
   b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.
   c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

      Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

      Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.
   d) Utilisez une des méthodes suivantes :
      - Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.

- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

6) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

   a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

   b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

   c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

   d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

   e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

7) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**

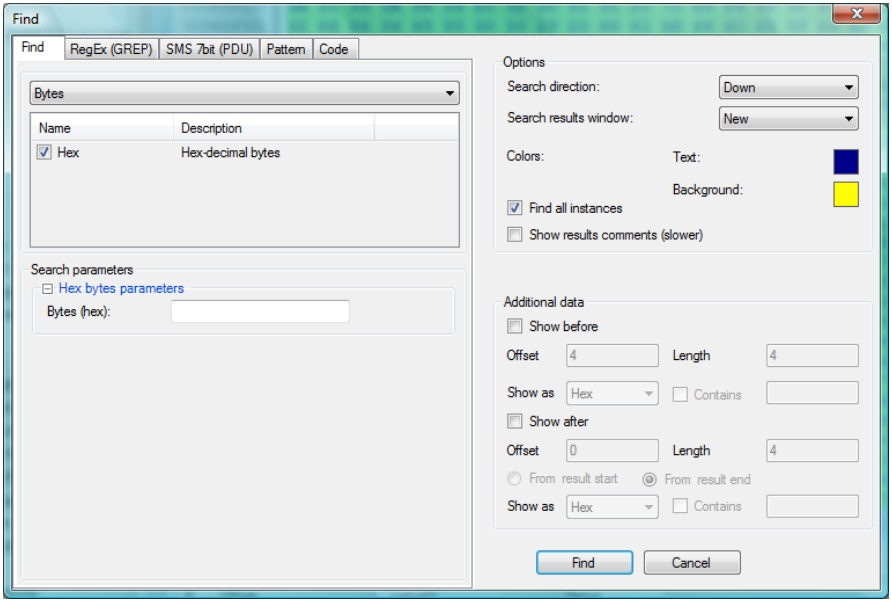
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

8) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
9) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
10) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel, HTML, PDF ou XML.

12.1.2. Rechercher des octets

Recherchez des octets pour trouver des occurrences spécifiques dans les données hexadécimales. Cette option est particulièrement utile lorsque vous connaissez l'en-tête d'identification d'un type de fichier ou d'une information que vous recherchez. Par exemple, les premiers octets hexadécimaux d'une image au format JPEG sont **FF D8 FF**. Ainsi, en recherchant **FF D8 FF**, les résultats fournissent l'emplacement de tous les en-têtes d'images au format JPEG possibles dans les données hexadécimales.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Dans l'onglet **Rechercher**, sélectionnez **Octets** dans la liste de types de données.



3) Sélectionnez **Hexadécimaux**.

L'écran **Paramètres de recherche** s'affiche :

4) Dans le champ **Octets (hexadécimaux)**, saisissez la valeur hexadécimale, par exemple **FFD8FF**.
5) Dans la zone **Options** , choisissez les options de recherche souhaitées :
    a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.
    b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.
    c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

    Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

    Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.
    d) Utilisez une des méthodes suivantes :
        - Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
        - Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

6) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

   a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

   b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

   c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

   d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

   e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

   f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

7) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**

- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

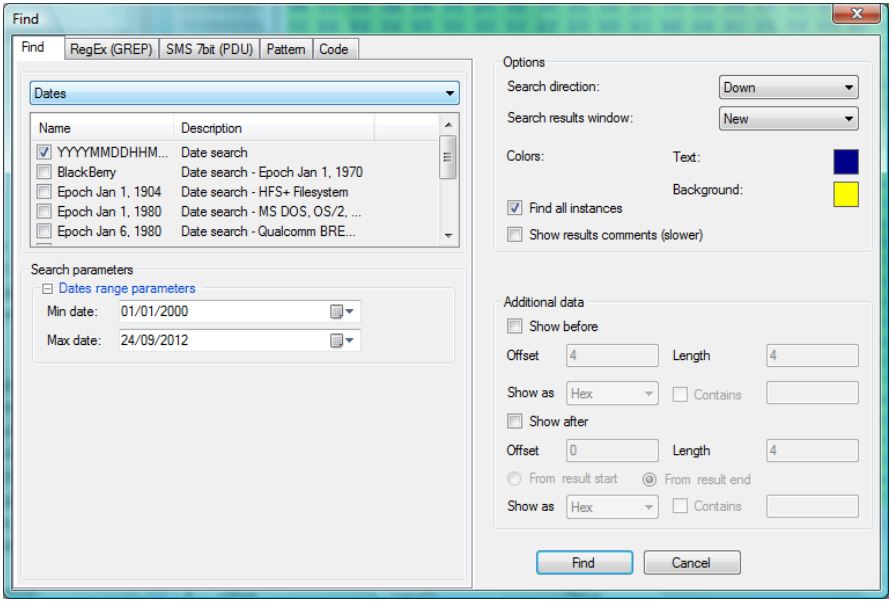
8) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
9) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
10) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel, HTML, PDF ou XML.

12.1.3. Rechercher des dates

Recherchez des dates pour trouver des périodes dans les données hexadécimales.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».

2) Dans l'onglet **Rechercher**, sélectionnez **Dates** dans la liste de types de données.



La fenêtre Filtres affiche une liste de formats de date et de plug-ins pouvant être utilisés pour rechercher des dates.

3) Sélectionnez le ou les formats de date et les plug-ins que vous souhaitez utiliser pour la recherche en cours.

REMARQUE : Les plug-ins adaptés varient selon l'encodage des données, le type d'appareil analysé, etc. Si vous sélectionnez un plug-in qui n'est pas adapté, vos résultats de recherche risquent de contenir de faux résultats. Par exemple, vous pouvez sélectionner **BlackBerry** si vous analysez un appareil BlackBerry. Si vous n'analysez pas un appareil BlackBerry et que vous sélectionnez **BlackBerry**, les résultats obtenus risquent d'être incorrects.

L'écran **Paramètres de recherche** s'affiche :

4) Dans les champs **Date min.** et **Date max.**, cliquez sur pour sélectionner une date sur le calendrier.

   Conseil : Choisissez une période courte pour limiter le nombre de résultats obtenus.

   Conseil : Lorsque vous recherchez une date précise, remplissez les champs **Date min.** et **Date max.** de façon à définir une période d'au moins 24 heures.

5) Dans la zone **Options** , choisissez les options de recherche souhaitées :

   a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.

   b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.

   c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

d) Utilisez une des méthodes suivantes :

- Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

6) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

7) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

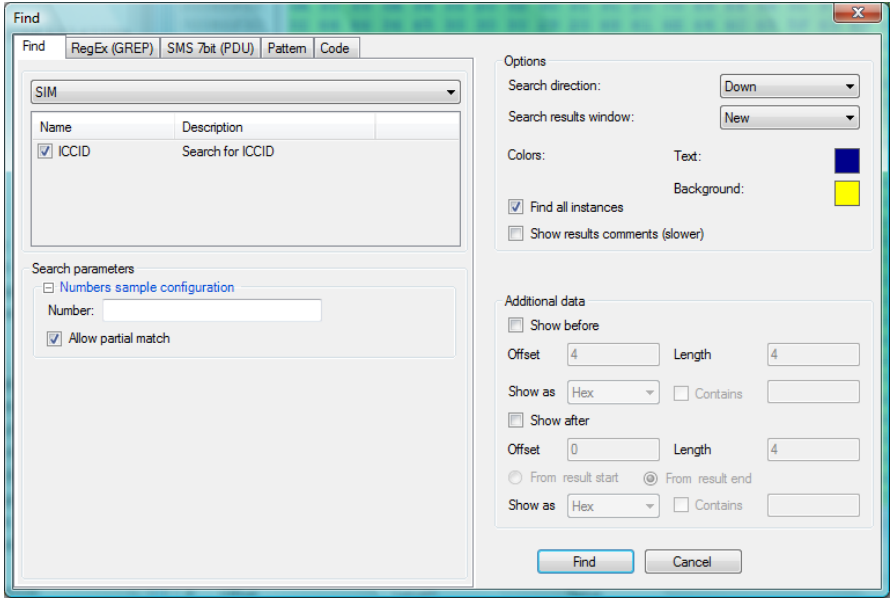
- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

8) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
9) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
10) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.4. Rechercher des numéros SIM ICCID

Cette méthode de recherche vous permet de trouver des numéros SIM ICCID dans les données hexadécimales.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Dans l'onglet **Rechercher**, sélectionnez **SIM** dans la liste de types de données.



3) Sélectionnez **ICCID**.

   L'écran **Paramètres de recherche** s'affiche :

4) Dans la zone Configuration de l'échantillon de numéros, saisissez le numéro ICCID dans le champ **Numéro**.

5) Si vous saisissez seulement une partie du numéro, sélectionnez **Autoriser les correspondances partielles**. Par exemple, si vous saisissez le nombre **89972** et que vous sélectionnez cette option, UFED Physical Analyzer recherche les numéros ICCID fournis par un fournisseur de services israélien.
6) Dans la zone **Options** , choisissez les options de recherche souhaitées :
    a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.
    b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.
    c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

    Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

    Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.
    d) Utilisez une des méthodes suivantes :
        - Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.

- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

7) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

   a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

   b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

   c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

   d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

   e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

8) Cliquez sur **Rechercher**.

REMARQUE : Si le champ **Numéro** est laissé vide, les résultats de recherche incluent tous les numéros correspondant au format ICCID.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.

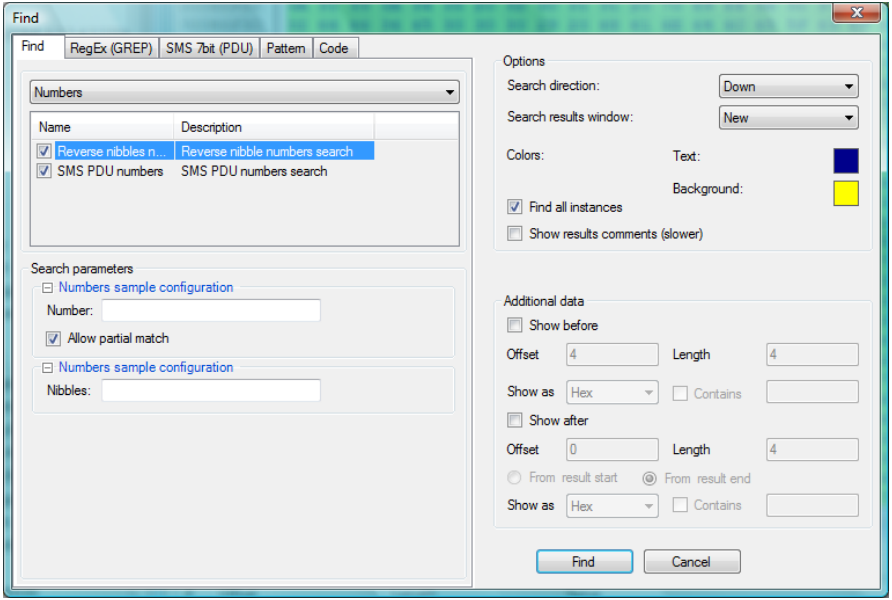
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

9) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
10) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
11) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.5. Rechercher des numéros SMS

Recherchez des numéros SMS dans les données hexadécimales.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Dans l'onglet **Rechercher**, sélectionnez **Numéros** dans la liste de types de données.



3) Pour rechercher des numéros SMS PDU, sélectionnez **Numéros SMS PDU**.

   L'écran **Paramètres de recherche** s'affiche :

   a) Dans le champ **Numéro** , sélectionnez le numéro à rechercher.

REMARQUE : Si le champ **Numéro** est laissé vide, les résultats de recherche incluent tous les numéros correspondant au format Numéro SMS.

b) Si vous saisissez seulement une partie du numéro, sélectionnez **Autoriser les correspondances partielles**.

4) Pour rechercher des quartets inversés, sélectionnez **Numéros quartets inversés**.

REMARQUE : Utilisez cette option lorsque les données ont été encodées pour inclure des quartets inversés.

L'écran **Paramètres de recherche** s'affiche :

- Dans le champ **Quartets** , sélectionnez le quartet à rechercher.

5) Dans la zone **Options** , choisissez les options de recherche souhaitées :

a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.

b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.

c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

d) Utilisez une des méthodes suivantes :

- Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

6) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

7) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

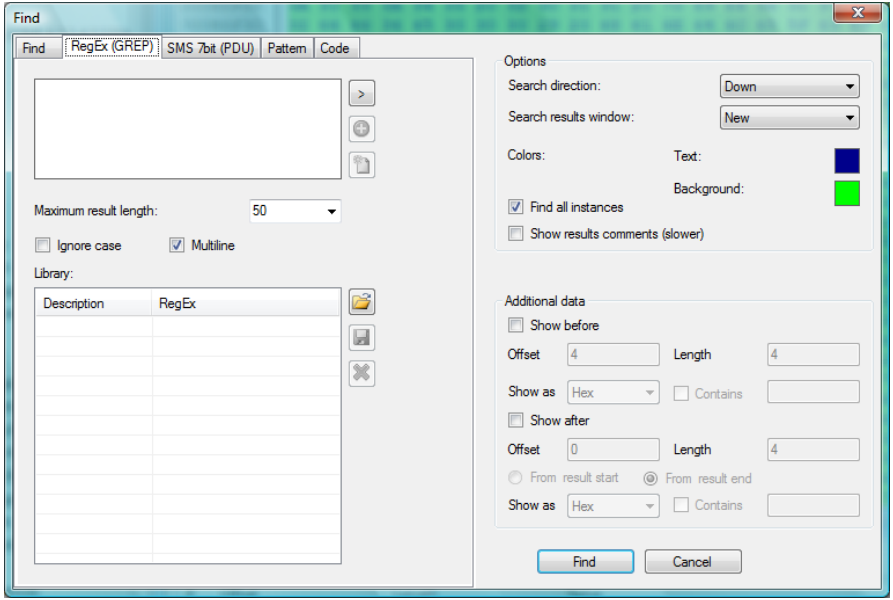
8) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
9) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
10) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.6. Rechercher des expressions régulières (GREP)

Recherchez des expressions régulières (RegEx) pour rechercher une structure de chaîne spécifique dans les données.

Par exemple, pour l'expression régulière « **[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[A-Za-z]{2,4}** », UFED Physical Analyzer recherche dans vos données toutes les adresses e-mail qui correspondent à la structure **<chaîne>@<chaîne>.<2 à 4 lettres>**.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».



2) Dans l'onglet **RegEx (GREP)**, saisissez l'expression que vous souhaitez utiliser dans la recherche.

3) Cliquez sur pour saisir un code d'expression régulière choisi dans une liste de codes communs.

4) Cliquez sur pour enregistrer l'expression actuelle dans la liste de la bibliothèque.

5) Cliquez sur pour effacer le champ de l'expression régulière.
6) Définissez la valeur **Longueur maximale du résultat** pour filtrer uniquement les résultats jusqu'à la longueur spécifiée.
7) Sélectionnez **Ignorer la casse** pour ignorer la casse dans les résultats de recherche.
8) Sélectionnez **Multiligne**.
9) Pour utiliser une expression enregistrée dans la bibliothèque, cliquez sur celle-ci dans la zone **Bibliothèque**.
10) Pour exporter la bibliothèque d'expressions régulières actuelle vers un fichier *.rel, cliquez sur .
11) Pour charger une expression régulière exportée depuis un fichier *.rel, cliquez sur .
12) Pour supprimer une expression de la liste de la bibliothèque, cliquez sur .
13) Dans la zone **Options** , choisissez les options de recherche souhaitées :
    a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.
    b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.
    c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

d) Utilisez une des méthodes suivantes :

- Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

14) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

15) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

16) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.

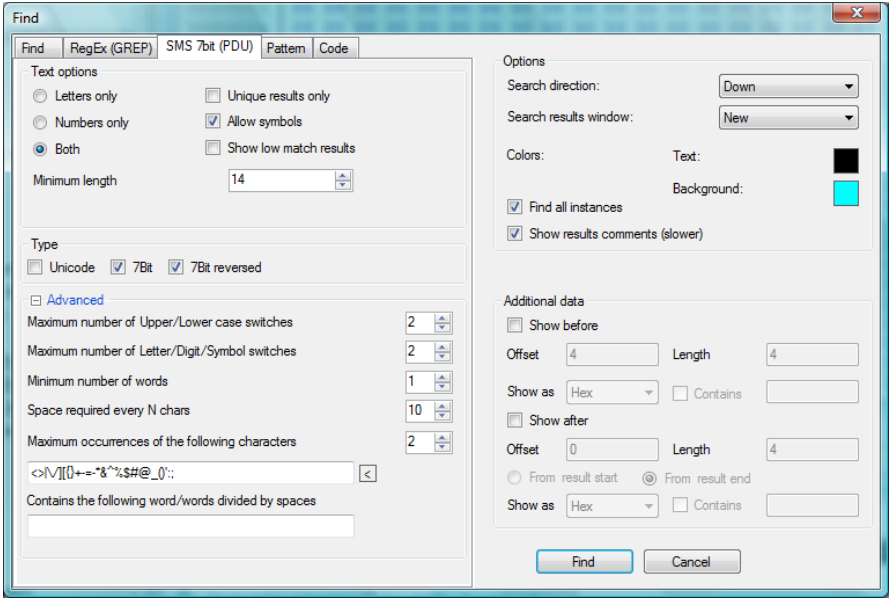
17) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.

18) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.7. Rechercher des chaînes de texte de SMS

Cette méthode de recherche vous permet de rechercher les chaînes de texte SMS (7 bits PDU) dans les données hexadécimales.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Sélectionnez l'onglet **SMS 7 bits (PDU)**.



3) Dans la zone **Options du texte**, définissez les paramètres de recherche suivants :
    a) Définissez le type de recherche : **Lettres seulement**, **Nombres seulement** ou **Les deux**.
    b) Pour afficher les résultats uniques, sélectionnez **Résultats uniques seulement**.

c) Pour autoriser les symboles dans les résultats de recherche, sélectionnez **Autoriser les symboles**.

d) Pour afficher les résultats avec une faible correspondance, sélectionnez **Afficher les résultats à correspondance faible**.

e) Pour définir le nombre minimum de caractères dans les résultats, définissez la **Longueur minimum**.

4) Dans la zone **Type**, sélectionnez le type de recherche : **Unicode**, **7 bits**, **7 bits inversés**.

5) Dans la zone **Avancé**, définissez les options suivantes, le cas échéant :

- **Nombre maximal de changements minuscule/majuscule**
- **Nombre maximal de changements Lettre/Chiffre/Symbole**
- **Nombre minimal de mots**
- **Espace requis tous les N caractères**
- **Nombre maximal d'occurrences des caractères suivants**
- **Contient le ou les mots suivants séparés par des espaces**.

6) Dans la zone **Options** , choisissez les options de recherche souhaitées :

a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.

b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.

c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

d) Utilisez une des méthodes suivantes :

- Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
- Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

7) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

8) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

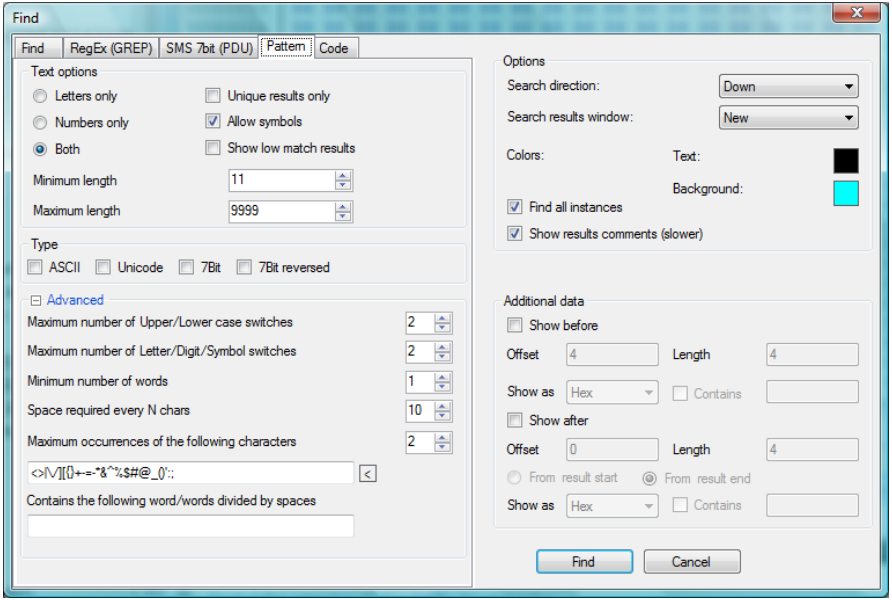
- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

9) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
10) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
11) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.8. Rechercher des schémas

Lorsque vous travaillez dans une structure de mémoire de taille importante, recherchez des schémas pour localiser tout contenu de nature textuelle.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Sélectionnez l'onglet **Schéma**.



3) Dans la zone **Options du texte**, définissez les paramètres de recherche suivants :
    a) Définissez le type de recherche : **Lettres seulement**, **Nombres seulement** ou **Les deux**.
    b) Pour afficher les résultats uniques, sélectionnez **Résultats uniques seulement**.

c) Pour autoriser les symboles dans les résultats de recherche, sélectionnez **Autoriser les symboles**.

d) Pour afficher les résultats avec une faible correspondance, sélectionnez **Afficher les résultats à correspondance faible**.

4) Dans les champs **Longueur minimale** et **Longueur maximale**, définissez la plage de longueurs du schéma.

   Cette option vous permet de filtrer les résultats en fonction des schémas recherchés.

5) Dans la zone **Type**, sélectionnez le type de recherche : **ASCII**, **Unicode**, **7 bits** et/ou **7 bits inversés**.

6) Dans la zone **Avancé**, définissez les options suivantes, le cas échéant :

   - **Nombre maximal de changements minuscule/majuscule**
   - **Nombre maximal de changements Lettre/Chiffre/Symbole**
   - **Nombre minimal de mots**
   - **Espace requis tous les N caractères**
   - **Nombre maximal d'occurrences des caractères suivants**
   - **Contient le ou les mots suivants séparés par des espaces**.

7) Dans la zone **Options** , choisissez les options de recherche souhaitées :

   a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.

   b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.

   c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

      Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

      Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

   d) Utilisez une des méthodes suivantes :

      - Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
      - Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

   e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

8) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

    a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

    b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

    c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

    d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

    e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

    f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

    g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

9) Cliquez sur **Rechercher**.

REMARQUE : La recherche de modèle peut être utilisée pour localiser tous les résultats possibles de texte de SMS à 7 bits. Pour limiter le nombre de faux résultats positifs, choisissez une plus grande valeur pour la **Longueur minimale**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**

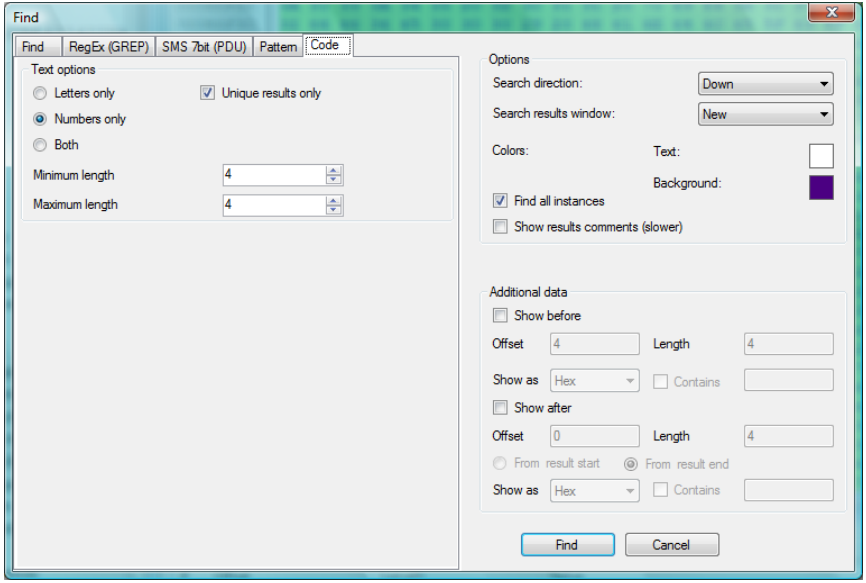
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.
- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

10) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
11) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
12) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.1.9. Rechercher des codes et des mots de passe

Recherchez des codes et des mots de passe utilisateur dans des structures de mémoire de taille importante.

1) Lorsque les données hexadécimales sont affichées, cliquez sur pour ouvrir la fenêtre « Rechercher ».
2) Sélectionnez l'onglet **Code**.



3) Dans la zone **Options du texte**, définissez les paramètres de recherche suivants :
    a) Définissez le type de recherche : **Lettres seulement**, **Nombres seulement** ou **Les deux**.
    b) Pour afficher les résultats uniques, sélectionnez **Résultats uniques seulement**.
4) Dans les champs **Longueur minimale** et **Longueur maximale**, définissez la plage de longueurs du schéma.

Cette option vous permet de filtrer les résultats en fonction des schémas recherchés.

5) Dans la zone **Options** , choisissez les options de recherche souhaitées :

   a) Dans la liste **Direction de recherche**, sélectionnez la direction de recherche.

   b) Dans la liste **Fenêtre de résultats de recherche**, sélectionnez **Nouveaux**, **Remplacer actuels** ou **Ajouter aux résultats actuels**, au choix.

   c) Pour définir les couleurs du **Texte** et de l'**Arrière-plan**, cliquez sur la palette, sélectionnez la couleur souhaitée, puis cliquez sur **OK**.

   Les couleurs choisies ici sont conservées pour la durée de la session. Pour modifier les couleurs par défaut, définissez-les dans la fenêtre Paramètres. Pour plus d'informations, consultez la section ***Paramètres de la visionneuse hexadécimale*** (page ***353***).

   Conseil : Pour distinguer facilement les résultats donnés pour chaque recherche effectuée, définissez des couleurs de texte et d'arrière-plan différentes pour chaque recherche.

   d) Utilisez une des méthodes suivantes :

   - Sélectionnez **Rechercher toutes les instances** pour afficher tous les résultats de la recherche à la fin du processus.
   - Décochez **Rechercher toutes les instances** pour afficher les éléments trouvés un par un au cours de la recherche (vous pouvez également appuyer sur F3 pour cela).

   e) Sélectionnez **Afficher les commentaires des résultats** pour afficher ceux-ci.

6) Dans la zone **Données supplémentaires**, améliorez vos capacités de recherche en ajoutant un nombre prédéfini de caractères avant et/ou après la valeur recherchée. Cela peut permettre de localiser des résultats spécifiques, ou même de limiter les résultats à des entités spécifiques de la valeur recherchée.

    a) Sélectionnez **Montrer avant** pour afficher les données qui se trouvent juste avant ce que vous recherchez.

    b) Dans le champ **Décalage**, saisissez le décalage avec le début du résultat de recherche à partir duquel les données supplémentaires doivent être incluses.

    c) Dans le champ **Longueur**, saisissez la longueur des données supplémentaires à ajouter à partir du point de décalage défini. Pour **Montrer avant**, la **Longueur** ne peut pas être supérieure au **Décalage**.

    d) Dans le champ **Afficher comme**, saisissez le type de données pour les données supplémentaires à afficher (**Hexadécimales**, **ASCII**, **Unicode** ou **7 bits**).

    e) Sélectionnez **Contient**, et saisissez une chaîne qui doit être contenue dans les données supplémentaires du résultat de recherche.

    f) Sélectionnez **Montrer après** pour afficher les données qui se trouvent juste après ce que vous recherchez, et répétez les étapes 2 à 5.

    g) Pour l'option **Montrer après**, choisissez si le décalage et la longueur des données supplémentaires sont calculés **À partir du début des résultats** ou **À partir de la fin des résultats**.

Les données supplémentaires sont consignées dans les champs **Données supplémentaires avant** et **Données supplémentaires après** des résultats de recherche.

7) Cliquez sur **Rechercher**.

Si vous avez sélectionné **Rechercher toutes les instances** dans la zone **Options**, les résultats s'affichent dans l'onglet **Résultats de recherche** dans l'onglet Informations sur l'analyse (dans l'onglet Vue hexadécimale).

Si vous n'avez pas sélectionné **Rechercher toutes les instances** dans la zone **Options**, la prochaine instance trouvée est mise en évidence dans l'onglet Vue hexadécimale.

L'onglet **Résultats de recherche** inclut les informations suivantes :

- **N°** – numéro de l'instance.
- **Décalage** – décalage d'adresse du fichier de données dans les données hexadécimales.
- **Longueur** – longueur de la chaîne en octets.
- **Valeur** – la chaîne elle-même.
- **Source**
- **Plus**
- **Données supplémentaires avant** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste avant le résultat.

- **Données supplémentaires après** – si vous sélectionnez l'option « Données supplémentaires » dans la fenêtre « Rechercher », les résultats affichent les données situées juste après le résultat.

8) Pour afficher une instance d'un résultat dans l'onglet Vue hexadécimale, cliquez sur la ligne souhaitée dans l'onglet Résultats de recherche.
9) Pour rechercher des données spécifiques et filtrer les résultats de recherche, utilisez le champ **Rechercher** dans l'onglet Résultats de recherche.
10) Pour exporter la liste des résultats de recherche, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

12.2. Parcourir l'extraction hexadécimale

- Double-cliquez sur une extraction hexadécimale dans l'arborescence de projet pour afficher son contenu dans un onglet Vue hexadécimale dans la zone d'affichage des données.

REMARQUE : Vous pouvez également cliquer sur les liens des images dans la zone Journal d'extraction en bas de l'onglet Résumé d'extraction pour accéder à l'extraction hexadécimale.

12.3. Utiliser un décalage pour accéder directement à un emplacement différent dans le fichier

Parcourez les données hexadécimales en définissant une valeur de décalage pour vous déplacer dans les données.

Pour vous déplacer depuis une position définie :

1) Cliquez sur .
2) Sélectionnez **Décimal** ou **Hexadécimal**, puis dans le champ **Décalage**, saisissez la valeur du décalage dans un format adapté.
3) Dans le champ **À partir de**, choisissez le point de référence à partir duquel le décalage est défini (**Début du fichier**, **Position actuelle** ou **Fin du fichier**).
4) Cliquez sur **Aller**.

   Le curseur se déplace jusqu'à l'emplacement décalé.

Pour vous déplacer depuis la position actuelle :

1) Cliquez sur un emplacement spécifique dans les données hexadécimales.
2) Dans le champ Valeur du décalage de la barre d'outils, saisissez la valeur de décalage souhaitée au format décimal (20) ou hexadécimal (0x20), ou sélectionnez une des valeur saisies précédemment dans la liste.

REMARQUE : Saisissez **+** ou **-** avant la valeur pour calculer le décalage à partir de la position actuelle.

3) Utilisez une des méthodes suivantes :
    - Cliquez sur pour vous déplacer vers l'arrière dans les données hexadécimales selon la valeur définie.
    - Cliquez sur pour vous déplacer vers l'avant dans les données hexadécimales selon la valeur définie.

12.4. Travailler avec les signets

Un signet est un pointeur de référence rapide que vous pouvez créer sur les données hexadécimales.

Les signets que vous créez sont gérés dans l'élément d'arborescence **Signets**. Le nombre de signets dans le projet apparaît entre parenthèses à côté de l'élément d'arborescence **Signets**.

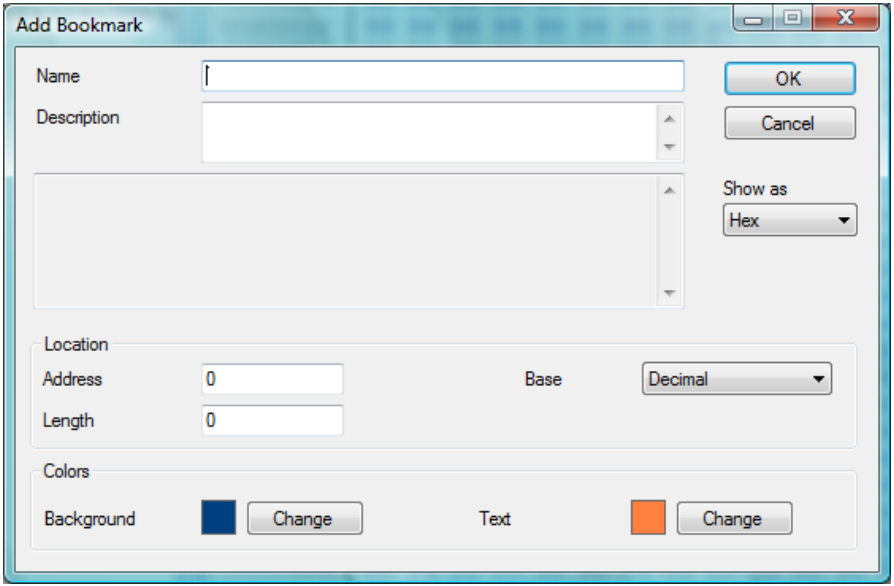
- Dans l'arborescence de projet, double-cliquez sur **Signets** pour ouvrir une liste des signets dans un onglet dans la zone d'affichage des données.
- Pour imprimer ou exporter la liste de signets d'entités, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Signets** : Excel , HTML , PDF ou XML .

12.4.1. Ajouter un signet

1) Lorsque les données hexadécimales sont affichées, sélectionnez une des options suivantes :
    - Dans la barre d'outils de l'onglet **Vue hexadécimale**, cliquez sur .

- Pour ajouter un signet à un segment spécifique dans les données hexadécimales, sélectionnez la section à laquelle vous souhaitez ajouter le signet, puis cliquez sur dans la barre d'outils de l'onglet Vue hexadécimale.
- Dans l'onglet **Signets**, cliquez sur .

La boîte de dialogue « Ajouter un signet » s'affiche.



2) Dans le champ **Nom**, saisissez le nom du signet.
3) Dans le champ **Description**, saisissez la description du signet.
4) Si vous n'avez sélectionné aucune zone dans les données hexadécimales, procédez de la façon suivante dans le champ **Emplacement** :
    a) Sélectionnez l'unité souhaitée pour l'adresse, **Décimale** ou **Hexadécimale**, dans la liste **Base**.
    b) Dans le champ **Adresse**, saisissez l'adresse du point de départ (décalage) des données auxquelles vous souhaitez ajouter un signet.
    c) Dans le champ **Longueur**, saisissez la longueur des données auxquelles vous souhaitez ajouter un signet.
5) Dans le champ **Couleurs**, définissez la couleur de l'arrière-plan et du texte pour le signet.
6) Cliquez sur **OK**.

    Le nouveau signet est enregistré et affiché dans l'onglet **Signets** de la vue hexadécimale.

    Le segment marqué est surligné avec les couleurs choisies. Les détails du signet s'affichent dans la fenêtre des résultats.

Chaque signet affiche les informations suivantes :

- **Décalage** – décalage d'adresse du paragraphe du signet dans les données hexadécimales.
- **Longueur** – longueur du segment de données auquel est attribué un signet.
- **Description** – nom du signet.

7) Cliquez sur un signet dans la liste des signets pour l'afficher dans la vue Hexadécimale.

12.4.2. Modifier un signet

1) Dans l'onglet **Signets** de la vue hexadécimale, cliquez sur .

   La boîte de dialogue « Ajouter un signet » s'affiche.

2) Modifiez le signet à votre convenance, puis cliquez sur **OK**.

12.4.3. Supprimer un signet

- Dans l'onglet **Signet** de la vue hexadécimale, sélectionnez le signet que vous souhaitez supprimer, puis cliquez sur .

  Le signet est supprimé.

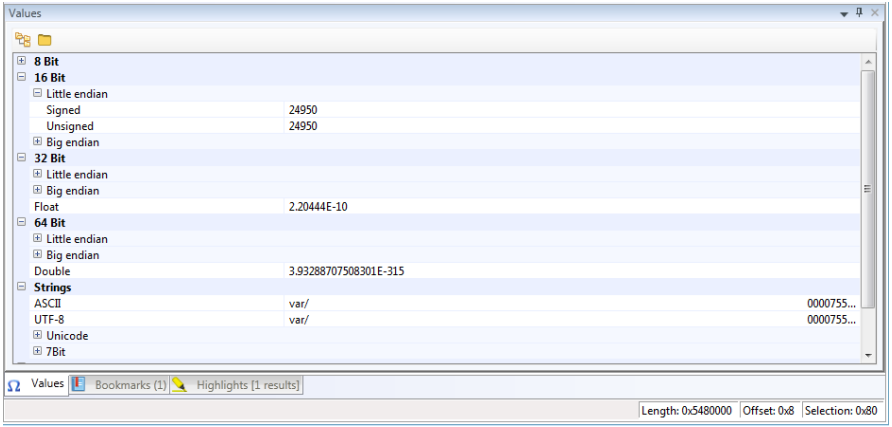
12.5. Décoder des données brutes

Sélectionnez des segments de données hexadécimales et décodez-les au fur et à mesure selon plusieurs types d'encodage.

UFED Physical Analyzer peut décoder les données hexadécimales vers les formats 8 bits, 16 bits, 32 bits, 64 bits, chaînes, date et heure, binaire et numérique.

Pour décoder des segments de données hexadécimales :

1) Dans l'onglet **Vue hexadécimale**, sélectionnez le segment de données que vous souhaitez décoder.
2) Dans l'onglet **Valeurs** en bas de l'onglet Vue hexadécimale, faites défiler les encodages jusqu'à celui que vous souhaitez, puis cliquez sur ⊞ pour agrandir la fenêtre.



REMARQUE : Certaines options d'encodage possèdent des catégories de sous-décodage.

3) Cliquez sur ou pour agrandir ou réduire tous les types d'encodage.
4) Pour décoder un segment de données différent, sélectionnez un segment différent dans l'onglet **Vue hexadécimale**.

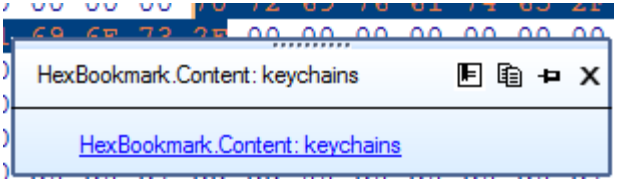
   Les résultats affichés dans l'onglet **Valeurs** changent pour correspondre au segment sélectionné.

12.6. Afficher les informations des données hexadécimales

Affichez les informations des segments mis en signet et des résultats de recherche lorsque vous les pointez dans l'onglet **Vue hexadécimale**.

1) Dans la barre d'outils de l'onglet Vue hexadécimale, cliquez sur .
2) Placez le curseur de la souris sur les informations mises en signet ou les résultats de recherche dans les données hexadécimales.

   Une fenêtre d'information flottante apparaît.



   Elle contient les informations suivantes :

   - Liens (pointeurs) vers les éléments de données analysés, tels que les fichiers et dossiers dans l'arborescence de projet.
   - Résultats de recherche associés aux données pointées.

3) Pour modifier le signet, cliquez sur .
4) Pour copier les données, cliquez sur .

Les données sont copiées sur le presse-papier.

5) Pour maintenir ouverte la fenêtre d'information, cliquez sur .

   La fenêtre d'information reste ouverte et affiche les informations relatives au dernier segment que vous pointez. Les informations affichées sur la fenêtre sont automatiquement mises à jour lorsque vous pointez le curseur de la souris sur un segment mis en signet ou un résultat de recherche différent.

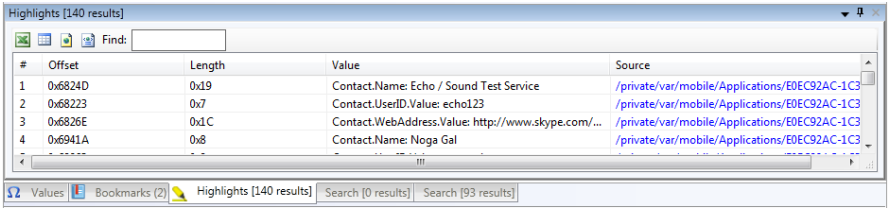
6) Pour fermer la fenêtre d'information, cliquez sur .

12.7. Localiser des types de données spécifiques dans les données hexadécimales

L'onglet **Mises en évidence** présente les emplacements des données analysées au sein des données hexadécimales, ce qui vous permet de déterminer le ou les emplacements exacts d'un type particulier de données analysées dans les données hexadécimales.

1) L'onglet **Mises en évidence** se trouve en bas de l'onglet Vue hexadécimale.
2) Dans l'arborescence de projet, sélectionnez un des dossiers **Données analysées** (par exemple **Contacts**).

Le dossier sélectionné est mis en évidence dans l'onglet **Vue hexadécimale**, et la liste des tranches de données qui composent le dossier se trouve dans l'onglet **Mises en évidence**.


Highlights [140 results]
Find:
Offset Length Value Source
1 0x6824D 0x19 Contact.Name: Echo / Sound Test Service /private/var/mobile/Applications/E0EC92AC-1C3
2 0x68223 0x7 Contact.UserID.Value: echo123 /private/var/mobile/Applications/E0EC92AC-1C3
3 0x6826E 0x1C Contact.WebAddress.Value: http://www.skype.com/... /private/var/mobile/Applications/E0EC92AC-1C3
4 0x6941A 0x8 Contact.Name: Noga Gal /private/var/mobile/Applications/E0EC92AC-1C3
Values
Bookmarks (2)
Highlights [140 results]
Search [0 results]
Search [93 results]

3) Pour exporter la liste des mises en évidence, cliquez sur le format souhaité dans la barre d'outils de l'onglet **Recherche** : Excel , HTML , PDF ou XML .

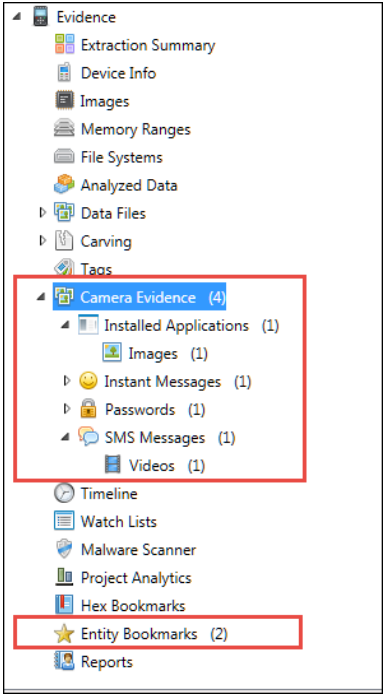
Chapitre 13 : **Preuve appareil photo et capture d'écran**

UFED 4PC ou UFED Touch associé à l'appareil photo UFED vous permet de rassembler des preuves en prenant des photos ou des vidéos d'un appareil. Une fonction Captures d'écran permet d'effectuer des captures d'écran en interne directement à partir d'un appareil Blackberry, Android ou iOS. Ces options peuvent être utiles pour réunir des preuves complémentaires, ou lorsqu'il est impossible d'extraire les données d'un appareil. Ces preuves peuvent être affichées dans UFED Physical Analyzer ainsi que des notes, catégories et signets ajoutés par l'examinateur. Pour plus d'informations sur la capture de preuves appareil photo et captures d'écran, reportez-vous aux manuels de l'utilisateur *UFED 4PC* ou *UFED Touch*.

Pour importer des preuves appareil photo ou capture d'écran :

- Cliquez sur le fichier Evidence.ufd.

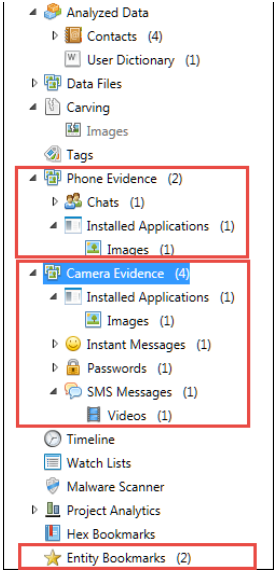
  Les preuves appareil photo (images et vidéos) ou les preuves téléphone (captures d'écran) sont importées dans UFED Physical Analyzer comme nouveau projet. Les preuves incluent les preuves téléphone ou les preuves appareil photo, séparées en catégories, ainsi que les signets d'entité et notes ajoutés au cours de l'extraction. En voici un exemple :



Pour importer des preuves appareil photo et capture d'écran avec les données extraites :

- Cliquez sur le fichier EvidenceCollection.ufdx.

Les preuves appareil photo (images et vidéos), les preuves téléphone (captures d'écran) et les données extraites sont importées dans UFED Physical Analyzer comme projet unique. Les preuves incluent les preuves téléphone ou les preuves appareil photo, ainsi que les catégories, signets d'entité et notes ajoutés au cours de l'extraction. En voici un exemple :

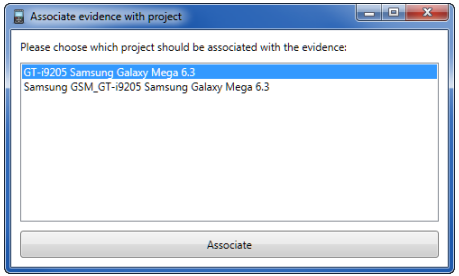


REMARQUE : Glissez-déposez le fichier EvidenceCollection.ufdx dans UFED Physical Analyzer pour ouvrir plusieurs extractions effectuées pour un appareil particulier. C'est-à-dire que toutes les extractions dans le dossier seront ouvertes. Chaque extraction (fichier .ufd) dans le dossier peut aussi être ouverte séparément. Un exemple de dossier avec plusieurs extractions et un fichier UFDX s'affiche ensuite.

Name
CaptureScreenshots 2014_08_27 (001) - Samsung GSM Samsung GT-i5510M Galaxy
FileSystemDump Samsung GSM GT-i5510M Galaxy 2014_08_27 (001)
Physical Samsung GSM GT-i5510M Galaxy 2014_08_27 (001)
UFED Samsung GSM GT-i5510M Galaxy 356210042118450 2014_08_27 (001)
EvidenceCollection.ufdx

Pour associer des preuves appareil photo et capture d'écran à un type d'extraction :

Si vous disposez de plusieurs types d'extraction ainsi que de preuves appareil photo, l'écran « Associer les preuves au projet » s'affiche.


Associate evidence with project
Please choose which project should be associated with the evidence:
GT-i9205 Samsung Galaxy Mega 6.3
Samsung GSM_GT-i9205 Samsung Galaxy Mega 6.3
Associate

- Sélectionnez l'extraction requise et cliquez sur **Associer**.

Chapitre 14 : **Décodage avancé**

14.1. Gérer les chaînes

Une chaîne est un ensemble de plug-ins regroupés et utilisés pour traiter les données extraites d'un appareil. Chaque appareil de la liste des appareils pris en charge par l'application dispose d'une chaîne d'analyse prédéfinie.

Une chaîne peut aussi être composée d'autres chaînes prédéfinies, inclues dans ses blocs de construction.

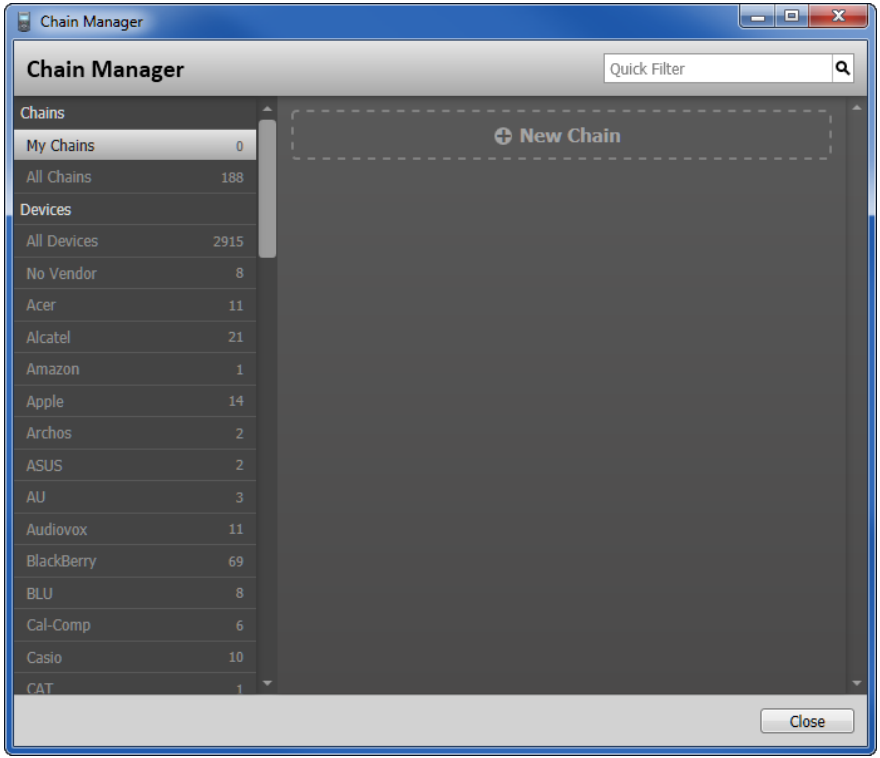
Utilisez le gestionnaire de chaînes pour :

- Gérer et modifier des chaînes existantes ;
- Créer des chaînes ;
- Affecter des chaînes à des appareils.

Pour gérer les chaînes d'application :

1) Utilisez une des méthodes suivantes :
    - Dans le menu **Plug-ins**, sélectionnez **Gestionnaire de chaînes**.
    - Cliquez sur .

L'écran Gestionnaire de chaînes s'affiche.



La liste de **Chaînes** sur la gauche vous permet de filtrer la liste de chaînes affichée.

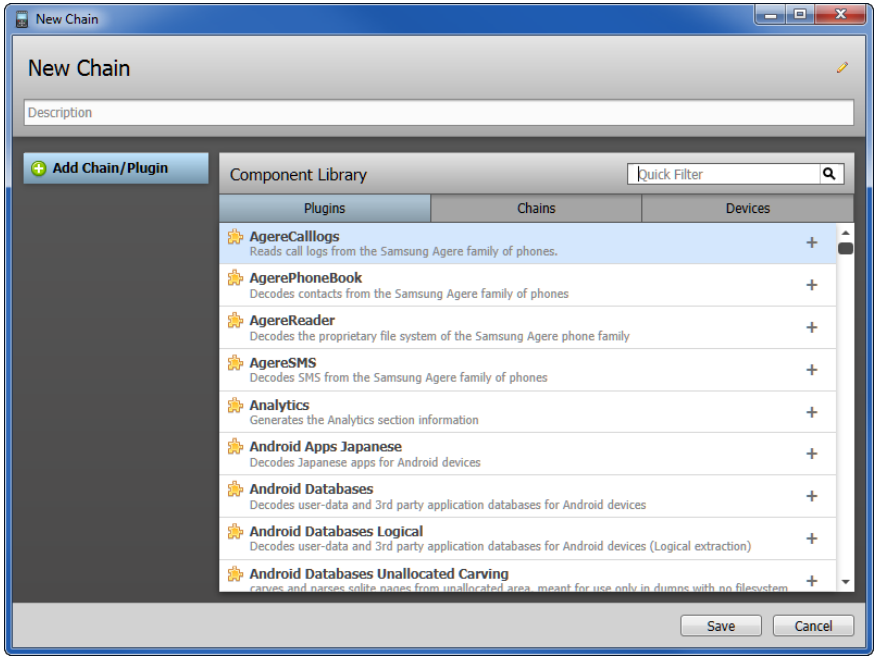
2) Cliquez sur **Mes chaînes** pour afficher vos chaînes personnalisées.
3) Cliquez sur **Toutes les chaînes** pour afficher une liste de toutes les chaînes prédéfinies.
4) Utilisez le **Filtre rapide** en haut à gauche de la fenêtre pour filtrer la liste de chaînes affichée.
5) Pour afficher les chaînes affectées à un appareil spécifique, sélectionnez une des options suivantes dans la section Appareils de la liste :
    - **Tous les appareils** pour afficher une liste de tous les appareils prédéfinis.
    - Le nom d'un fabricant, pour afficher une liste des appareils prédéfinis du fabricant sélectionné.
6) Double-cliquez sur un appareil pour afficher sa fenêtre Chaînes.

   La fenêtre Chaînes de l'appareil affiche au moins une chaîne qui lui est attribuée.

14.1.1. Construire une chaîne

1) Dans la fenêtre Gestionnaire de chaînes, cliquez sur **Nouvelle chaîne**.
2) Cliquez sur **Nouvelle chaîne**.

L'écran Nouvelle chaîne s'affiche.



3) Cliquez sur **Nouvelle chaîne** en haut de la fenêtre, puis saisissez un nom pour la chaîne.
4) Dans le champ **Description**, saisissez une courte description de la chaîne (facultatif).

5) Dans la bibliothèque de composants, sélectionnez une catégorie de composants :
    - **Plug-ins** – des plug-ins spécifiques.
    - **Chaînes** – chaîne prédéfinie spécifique.
    - **Appareils** – chaîne complète d'un plug-in spécifique.

    REMARQUE : Les **Appareils** et les **Chaînes** sont ajoutés à la chaîne comme composant de celle-ci.

6) Pour ajouter un composant à la liste de votre chaîne, cliquez sur le + à côté du composant.
7) Pour supprimer un composant de la liste de la chaîne, cliquez sur le ✖ à droite du composant, puis sur **Oui** pour confirmer.
8) Pour modifier les paramètres d'un plug-in ou d'une chaîne, sélectionnez-le/la dans la liste des composants de la chaîne (sur la gauche) et définissez les options qui s'affichent.

    REMARQUE : Pour revenir à la bibliothèque de composants et continuer à ajouter des plug-ins et des chaînes, cliquez sur **Ajouter une chaîne/un plug-in**.

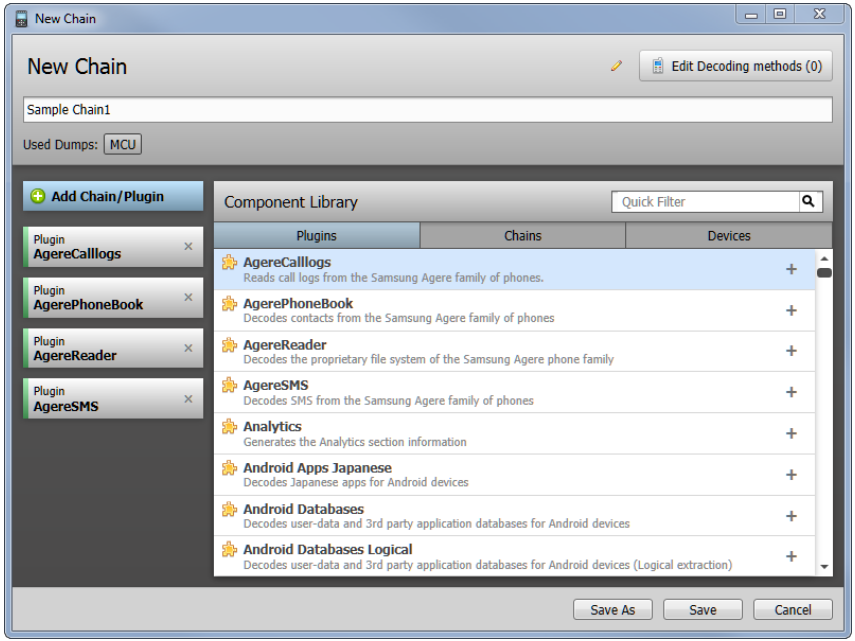
9) Lorsque vous avez terminé, cliquez sur **Enregistrer**.

    La nouvelle chaîne est ajoutée à votre liste Mes chaînes.

14.1.2. Modifier une chaîne existante

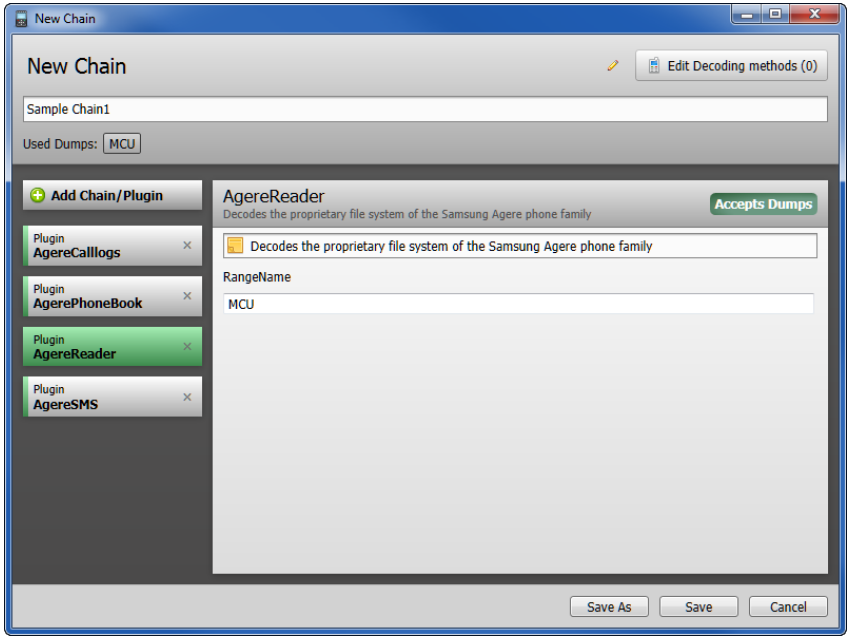
1) Modifiez les chaînes que vous avez créées.
2) Dans la liste **Mes chaînes** du Gestionnaire de chaînes, double-cliquez sur la chaîne que vous souhaitez modifier.

3) Cliquez sur **Ajouter une chaîne/un plug-in** pour afficher la bibliothèque de composants.



4) Pour ajouter un composant à la liste de votre chaîne, cliquez sur le + à côté du composant.
5) Pour supprimer un composant de la liste de la chaîne, cliquez sur le × à droite du composant, puis sur **Oui** pour confirmer.

6) Pour modifier les paramètres d'un plug-in ou d'une chaîne, sélectionnez-le/la dans la liste des composants de la chaîne (sur la gauche) et définissez les options qui s'affichent.



REMARQUE : Pour revenir à la bibliothèque de composants et continuer à ajouter des plug-ins et des chaînes, cliquez sur **Ajouter une chaîne/un plug-in**.

7) Lorsque vous avez terminé, cliquez sur **Enregistrer**, ou sur **Enregistrer sous** pour enregistrer la chaîne modifiée comme nouvelle chaîne.
8) Si vous avez cliqué sur **Enregistrer sous**, saisissez un nom pour la nouvelle chaîne, puis cliquez sur **Enregistrer**.

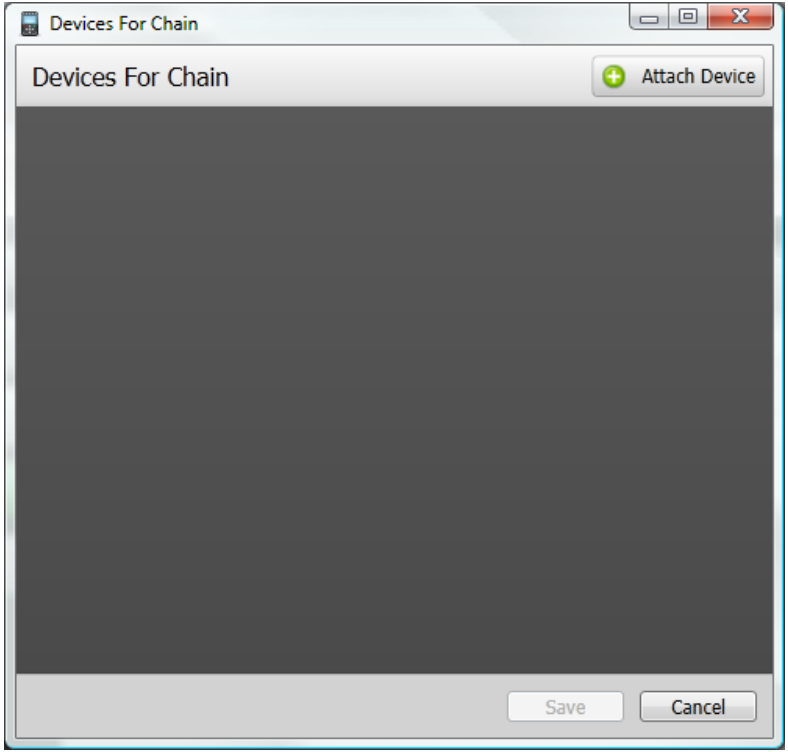
REMARQUE : Les modifications apportées aux chaînes verrouillées prédéfinies en usine ne peuvent être enregistrées que comme nouvelle chaîne.

14.1.3. Gérer les chaînes d'appareils

14.1.3.1. Associer des appareils à une chaîne

Vous pouvez associer des appareils à des chaînes que vous avez créées, ou modifier les chaînes d'appareils et les enregistrer comme copie.

1) Double-cliquez sur la chaîne à laquelle vous souhaitez associer un appareil.
2) Cliquez sur **Modifier les appareils**.



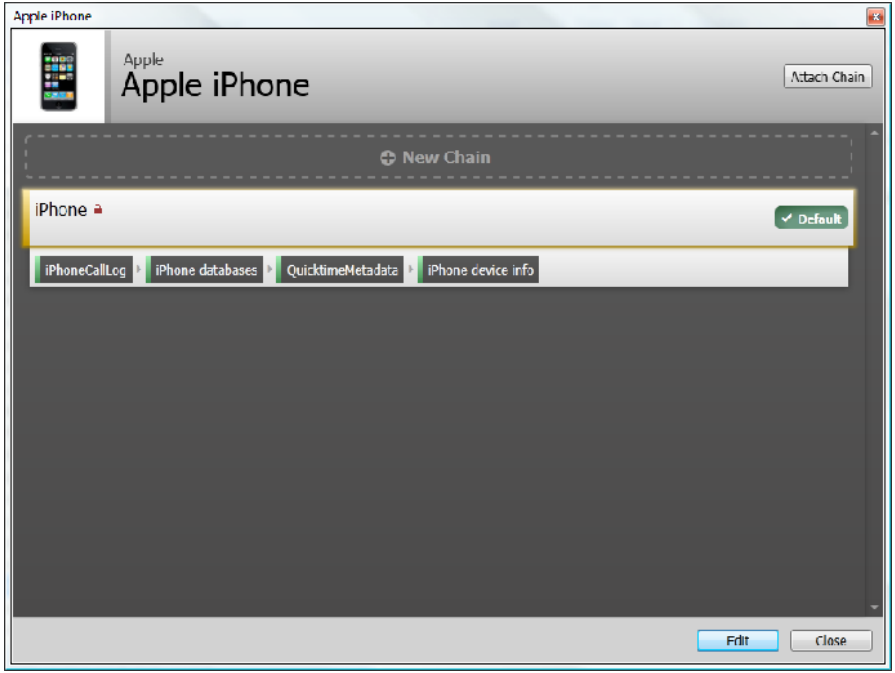
3) Dans la fenêtre Appareils pour la chaîne, cliquez sur **Associer l'appareil**.

4) Dans la fenêtre Sélectionner l'appareil, sélectionnez l'appareil que vous souhaitez associer à la chaîne.

5) Cliquez sur **Sélectionner**.
6) Répétez les étapes 3 à 5 pour ajouter des appareils supplémentaires.
7) Lorsque vous avez terminé d'associer des appareils, cliquez sur **Enregistrer**.

14.1.3.2. Définir la chaîne d'appareils par défaut

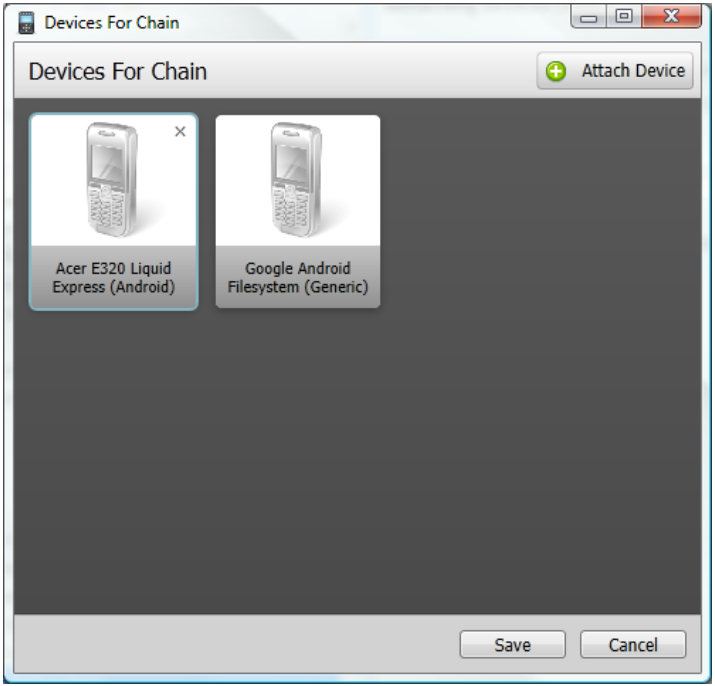
1) Dans la fenêtre Gestionnaire de chaînes, utilisez la liste des appareils pour localiser l'appareil que vous souhaitez modifier.
2) Double-cliquez sur l'appareil pour afficher sa fenêtre Chaînes.



3) Si la liste de chaînes de l'appareil contient plusieurs chaînes, cliquez sur pour la définir comme chaîne par défaut de l'appareil.
4) Cliquez sur **Fermer** pour fermer la fenêtre Chaînes de l'appareil.

14.1.3.3. Dissocier des appareils d'une chaîne

1) Double-cliquez sur la chaîne de laquelle vous souhaitez dissocier un appareil.
2) Cliquez sur **Modifier les appareils** dans l'angle supérieur droit de la fenêtre de la chaîne.



3) Cliquez sur le ✖ à droite de chaque appareil que vous souhaitez dissocier de la chaîne.
4) Cliquez sur **Fermer**.
5) Cliquez sur **Annuler** pour fermer la fenêtre Chaînes.

14.1.4. Supprimer une chaîne

Vous ne pouvez supprimer les chaînes que dans la liste Mes chaînes.

1) Dans la fenêtre Gestionnaire de chaînes, cliquez sélectionnez **Mes chaînes**.
2) Cliquez sur ✖ à droite de la chaîne.

14.1.5. Description des chaînes

Le tableau suivant répertorie les chaînes d'appareil UFED et leur description.

Nom de la chaîne	Description
AndroidContent	Décode le contenu pour les systèmes de fichiers Android.
AndroidContent Japanese	Décode le contenu pour les systèmes de fichiers Android et les applications japonaises.
AndroidFS	Décode différents systèmes de fichiers sur Android. Cette chaîne fait partie des chaînes `Motorola Android` ou `AndroidDD`.

Nom de la chaîne	Description
AndroidDD	Décode certains types d'appareils Android en utilisant les métadonnées de l'extraction.
AndroidDD Japanese	Décode certains types d'appareils Android et d'applications japonaises en utilisant les métadonnées de l'extraction.
AndroidiDen	Décode Motorola iDen avec Android utilisant les extractions physiques du système.
Android Logical with Content	Décode le contenu pour les extractions numériques Android.
AndroidMotorolaYaffs	Décode les extractions de l'appareil Motorola Android (`AndroidDD`).
AndroidMTK NAND	Décode les extractions NAND d'appareils MTK Android.
AndroidNvidia	Décode les appareils Android avec chipset Nvidia.
AndroidSamsungFAT	Décode plusieurs téléphones Samsung Android avec systèmes de fichiers FAT.
BlackBerryIPD	Décode les appareils de sauvegarde BlackBerry utilisant la chaîne par défaut de Cellebrite.
BlackBerry Physical	Décode les extractions physiques et/ou de systèmes de fichiers BlackBerry.
BlackBerryBackup	Décode les extractions de sauvegarde BlackBerry.
CasioC700Content	Décode les modèles pour la série Casio c7X1.
Generic FAT	Décode le système FAT (table d'allocation de fichier).
iCloudBackup	Décode les données de la sauvegarde Apple iCloud.

Nom de la chaîne	Description
iPhone Japanese Content	Décode le contenu pour les iPhones japonais.
iPhone Databases Logical	Décode le contenu iPhone pour les extractions numériques.
iPhoneBackupLogical	Décode les données des sauvegardes iPhone pour les extractions numériques.
iPhoneFS	Décode les systèmes de fichiers et le contenu sur iPhone.
iPhonePhysical	Décode les extractions physiques iPhone.
Motorola Android	Décode les appareils Motorola Android.
Nokia FS	Décode les systèmes de fichiers sur Nokia.
Nokia Content	Décode tout le contenu sur Nokia.
Nokia Predef XSR	Décode les extractions physiques non Symbian Nokia BB5.
PantechCdm8999Contents	Décode SMS, MMS et journaux d'appels pour l'appareil Pantech CDM8999.
QCAndroid	Décode les extractions physiques Qualcomm Android.
Qualcomm Winmobile	Décode la couche de traduction flash du mobile LG Windows et extrait les fichiers et SMS du système de fichiers.
Report	Décode les rapports dans UFED Physical Analyzer.
Samsung Qualcomm with Content	Décode le système de fichiers et le contenu des appareils Samsung Qualcomm.
Sanyo Qualcomm CDMA Physical	Décode les systèmes de fichiers et le contenu de la couche de traduction flash des appareils Sanyo CDMA avec puce Qualcomm.

Nom de la chaîne	Description
Symbian Physical	Décode la couche de traduction flash et une partition FAT à l'aide de Symbian.
WebOS	Décode les systèmes de fichiers pour les appareils avec système d'exploitation sur Internet (Palm).
WindowsPhone7	Décode les extractions des appareils Windows Phone 7.
AndroidXSR	Décode les appareils Android avec la couche de traduction flash XSR.
BlackBerry Filesystem Content	Décode les données des systèmes de fichiers BlackBerry.
Android Samsung Nexus	Décode les appareils Samsung Nexus.
AndroidMTK MMC	Décode les extractions MMC d'appareils MTK Android.
Samsung Non Android Content	Décode le contenu des appareils Samsung qui n'utilisent pas les systèmes d'exploitation Android.
Nokia Predef Content	Décode le contenu des appareils Nokia Predef.
Samsung MCUv2 - No MMS, Phonebook	Décode les appareils MCUv2 à l'exception des MMS et du répertoire téléphonique.
Samsung Qualcomm JTAG with Content	Décode le système de fichiers et le contenu des extractions JTAG des appareils Samsung Qualcomm.
Windows Mobile XSR JTAG	Décode les extractions JTAG des appareils Windows mobile avec la couche de traduction flash XSR.

Nom de la chaîne	Description
SIM Card FS	Décode le contenu des extractions de systèmes de fichiers de cartes SIM.
LG Qualcomm JTAG with Content	Décode le système de fichiers et le contenu des extractions JTAG des appareils LG Qualcomm.
Sanyo Qualcomm JTAG with Content	Décode le contenu des extractions JTAG des appareils Sanyo CDMA avec puce Qualcomm.
Samsung Generic JTAG	Décode les extractions avec toutes les méthodes prises en charge pour les appareils Samsung.
HTC Generic JTAG	Décode les extractions avec toutes les méthodes prises en charge pour les appareils HTC.
Samsung Qualcomm with SMS	Décode le système de fichiers et les SMS des appareils Samsung Qualcomm.
iPhone Logical with Content	Décode les extractions de rapport numérique iPhone.

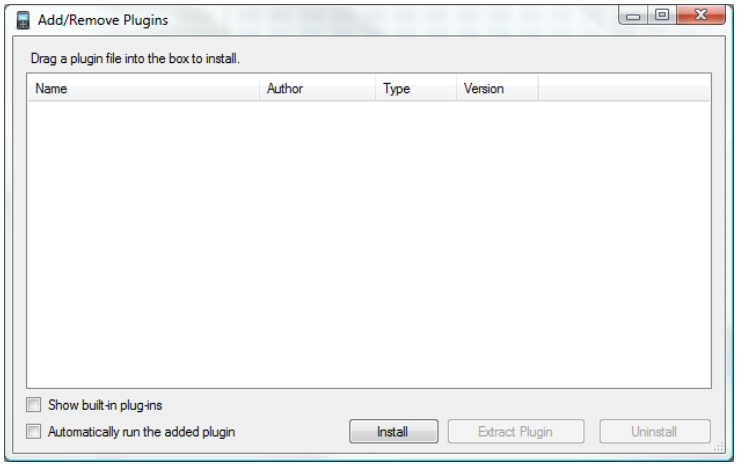
14.2. Plug-ins

Le mécanisme des plug-ins est une API qui permet aux utilisateurs d'augmenter les capacités de l'application en ajoutant des plug-ins fournis par Cellebrite ou des plug-ins personnalisés écrits à l'aide du shell Python.

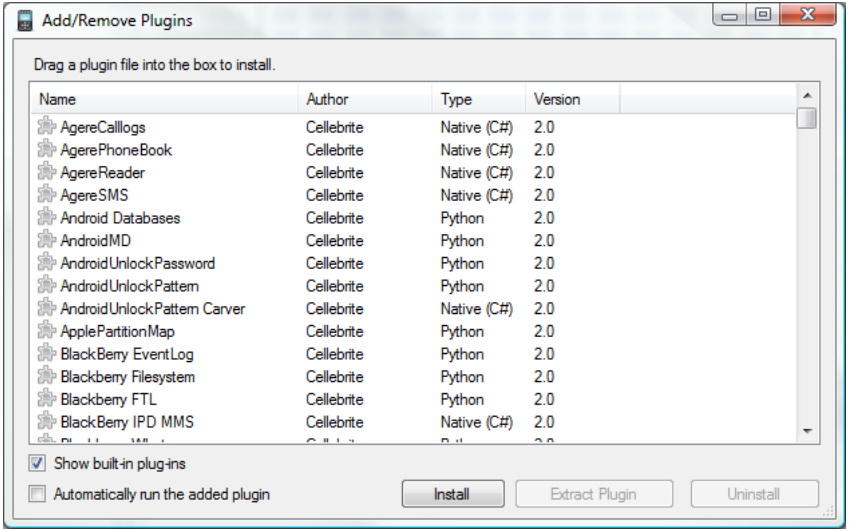
14.2.1. Gérer les plug-ins

La fenêtre Ajouter/Supprimer des plug-ins vous permet de gérer les plug-ins installés.

1) Cliquez sur .



2) Pour afficher les plug-ins installés, y compris les plug-ins intégrés qui ne peuvent pas être supprimés, sélectionnez **Afficher les plug-ins intégrés**.



Dans la fenêtre Ajouter/Supprimer des plug-ins, effectuez les tâches suivantes :

3) Pour installer des plug-ins supplémentaires, faites-les glisser sur la fenêtre Ajouter/Supprimer des plug-ins.
4) Pour extraire une copie d'un plug-in installé, sélectionnez-le et cliquez sur **Extraire le plug-in**.
5) Pour supprimer un plug-in installé, sélectionnez-le et cliquez sur **Désinstaller**.

REMARQUE : Vous ne pouvez pas extraire ou désinstaller un plug-in intégré de l'application.

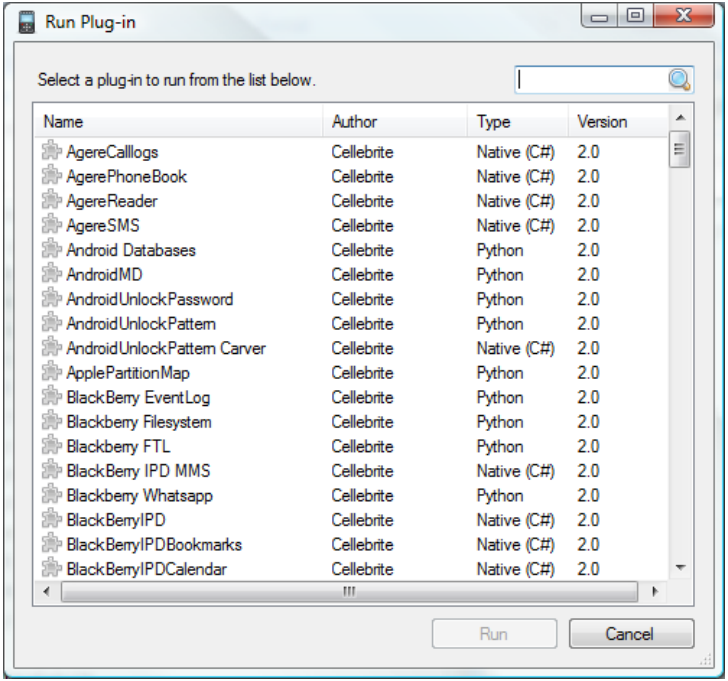
6) Pour afficher le statut d'un plug-in, double-cliquez sur celui-ci.

   La boîte de dialogue Statut du plug-in affiche son statut, qui peut être « Signé » ou « Non signé ».

   Un plug-in signé est un plug-in qui a été approuvé et signé par Cellebrite.

14.2.2. Exécuter un plug-in spécifique

1) Exécutez un plug-in individuel sur votre projet.
2) Dans le menu **Plug-ins**, sélectionnez **Exécuter un plug-in**.


Run Plug-in
Select a plug-in to run from the list below.
Name
Author
Type
Version
AgereCalllogs Cellebrite Native (C#) 2.0
AgerePhoneBook Cellebrite Native (C#) 2.0
AgereReader Cellebrite Native (C#) 2.0
AgereSMS Cellebrite Native (C#) 2.0
Android Databases Cellebrite Python 2.0
AndroidMD Cellebrite Python 2.0
AndroidUnlockPassword Cellebrite Python 2.0
AndroidUnlockPattern Cellebrite Python 2.0
AndroidUnlockPattern Carver Cellebrite Native (C#) 2.0
ApplePartitionMap Cellebrite Python 2.0
BlackBerry EventLog Cellebrite Python 2.0
Blackberry Filesystem Cellebrite Python 2.0
Blackberry FTL Cellebrite Python 2.0
BlackBerry IPD MMS Cellebrite Native (C#) 2.0
Blackberry Whatsapp Cellebrite Python 2.0
BlackBerryIPD Cellebrite Native (C#) 2.0
BlackBerryIPDBookmarks Cellebrite Native (C#) 2.0
BlackBerryIPDCalendar Cellebrite Native (C#) 2.0
Run
Cancel

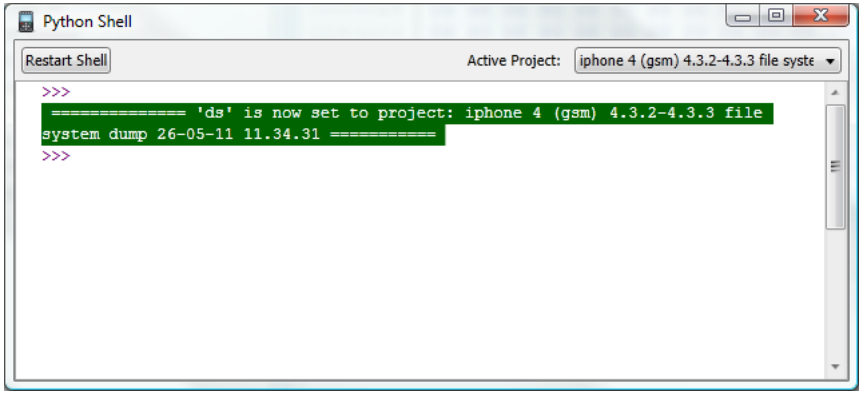
3) Sélectionnez le plug-in souhaité dans la liste, puis cliquez sur **Exécuter**.

14.3. Utiliser le shell Python

Le shell Python intégré vous permet d'exécuter un décodage et une analyse personnalisés en utilisant les commandes Python.

Pour ouvrir la fenêtre Shell Python, procédez de l'une des façons suivantes :

1) Dans le menu **Python**, sélectionnez **Shell Python**.
2) Cliquez sur .


Python Shell
Restart Shell
Active Project:
iphone 4 (gsm) 4.3.2-4.3.3 file syste
>>>
========== 'ds' is now set to project: iphone 4 (gsm) 4.3.2-4.3.3 file system dump 26-05-11 11.34.31 ==========
>>>

Pour en savoir plus sur l'utilisation des commandes du shell Python pour l'analyse personnalisée, consultez le « Guide d'écriture de script Python », disponible dans le menu **Aide**.

14.4. Exporter le système de fichiers

Exportez le système de fichiers extrait pour l'enregistrer en totalité à l'emplacement de votre choix sur votre ordinateur. Cet enregistrement conserve la même hiérarchie que la structure des dossiers et fichiers physiques du système de fichiers original.

Pour exporter le système de fichiers extrait :

1) Dans le menu **Outils**, sélectionnez **Vidage du système de fichiers** ou cliquez sur .
2) Dans la fenêtre de dialogue Parcourir les dossiers, sélectionnez l'emplacement où vous souhaitez enregistrer le système de fichiers extrait.
3) Cliquez sur **Créer un nouveau dossier** pour créer un dossier à l'emplacement cible.
4) Cliquez sur **OK** pour exporter le système de fichiers.

14.5. Utiliser le plug-in de reconstitution de schéma de déverrouillage Android

Utilisez le plug-in de reconstitution de schéma de déverrouillage Android lorsque vous travaillez avec des appareils Android pour lesquels le décodage n'est pas encore pris en charge.

Le plug-in de reconstitution de schéma de déverrouillage Android permet de décoder les schémas de déverrouillage sur les appareils Android. Ce plug-in peut être exécuté sur le fichier image créé par l'appareil UFED, JTAG, Chip-off, ou d'autres outils pour lesquels le décodage n'est pas encore pris en

charge. Le fichier image peut être composé de toutes les partitions de l'appareil, ou uniquement de la partition de données utilisateur.

1) Effectuez une extraction physique avec l'appareil UFED.
2) Dans UFED Physical Analyzer, ouvrez l'extraction physique Android par glisser-déposer ou en utilisant l'option « Ouverture avancée ».
3) Exécutez le plug-in **Reconstitution de schéma de déverrouillage Android**. Pour plus d'informations sur l'exécution d'un plug-in, consultez la section ***Exécuter un plug-in spécifique*** (page ***337***).

   Le schéma de déverrouillage est présenté dans l'onglet **Résumé d'extraction**, dans la zone **Infos appareil**.
4) Déverrouillez l'appareil Android et effectuez une extraction physique ou de système de fichiers avec l'appareil UFED.

14.6. Plug-in de reconstitution de mot de passe de déverrouillage Android

UFED Physical Analyzer inclut le plug-in de reconstitution de mot de passe de déverrouillage Android. Ce plug-in, développé par le groupe CCL Forensics et intégré dans UFED Physical Analyzer par Cellebrite, tente d'extraire les mots de passe de déverrouillage des extractions Android. Ce plug-in se trouve dans la liste des plug-ins standard.

Chapitre 15 : **Paramètres**

La fenêtre « Paramètres » permet d'accéder aux options de configuration fonctionnelles et comportementales utilisées pour ajuster et contrôler les fonctionnalités et l'utilisation de l'application. Les paramètres de la fenêtre « Paramètres » s'appliquent à tous les projets ouverts dans UFED Physical Analyzer.

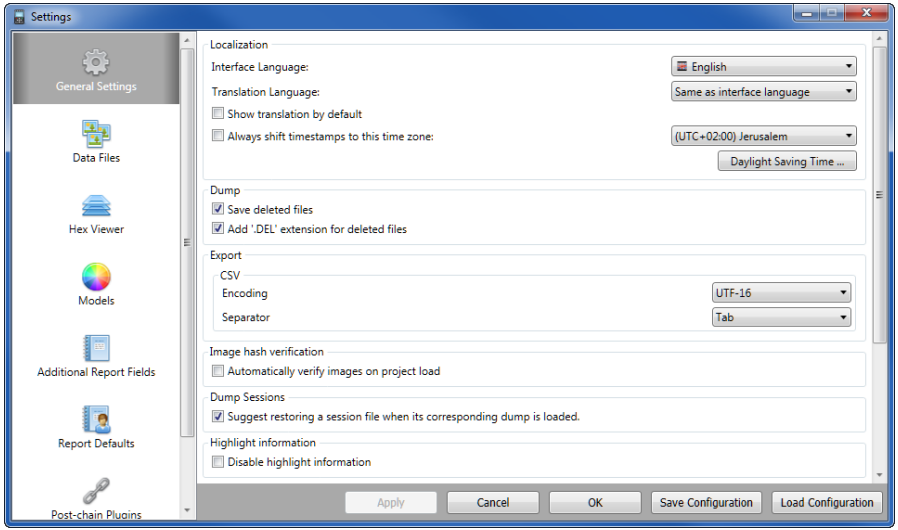
REMARQUE : Les modifications des paramètres sont perdues lorsque vous fermez UFED Physical Analyzer. Pour enregistrer la configuration des paramètres, consultez la section ***Enregistrer les paramètres*** (page ***371***).

- Pour accéder à la fenêtre « Paramètres », procédez de l'une des façons suivantes :
  - Sélectionnez **Outils** > **Paramètres.**
  - Cliquez sur .

  La fenêtre « Paramètres » s'affiche.

15.1. Paramètres généraux

Les paramètres généraux de l'application peuvent être définis dans l'onglet **Paramètres généraux**.



Pour configurer la langue de l'interface de UFED Physical Analyzer :

- Dans la liste **Langue**, sélectionnez la langue souhaitée.

Pour définir la langue de traduction :

1) Sélectionnez la langue de traduction. C'est la langue dans laquelle vous souhaitez traduire le texte. Vous ne pouvez sélectionner qu'une seule langue de traduction. Pour demandez des langues de traduction supplémentaires, sélectionnez **Plus de langues**.
2) Cochez la case **Afficher la langue de traduction par défaut** pour afficher les traductions par défaut. Décochez cette case pour que la traduction n'apparaisse pas lorsque vous traduisez le texte. Pour afficher la traduction, sélectionnez **Afficher la traduction**.

Pour déplacer les horodateurs vers un fuseau horaire particulier :

1) Dans la liste Paramètres de fuseau horaire (UTC), sélectionnez :
    - Valeur UTC originale pour afficher les horodateurs tels qu'ils ont été enregistrés (sans unification).
    - Un des fuseaux horaires (UTC -12:00 à UTC +13:00) pour recalculer les horodateurs définis par le réseau en fonction du décalage du fuseau horaire.
2) Pour modifier les dates de début et de fin de l'heure d'été, cliquez sur **Heure d'été**. Pour en savoir plus sur comment modifier les paramètres de fuseau horaire, reportez-vous à la section ***Définir un fuseau horaire unifié pour le projet*** *(page **372**)*.

Pour configurer la gestion des fichiers supprimés lors de l'utilisation de la fonctionnalité Vidage GPS/Appareil de stockage de masse :

1) Dans la zone **Vidage**, sélectionnez **Enregistrer les fichiers supprimés** pour enregistrer les fichiers supprimés.

2) Sélectionnez **Ajouter l'extension "DEL" aux fichiers supprimés**, pour enregistrer les fichiers supprimés avec l'extension *.DEL.

Pour configurer l'encodage et le séparateur des fichiers CSV exportés :

1) Dans la zone **Exporter**, sélectionnez l'option d'encodage souhaitée dans la liste **Encodage**.
2) Sélectionnez le séparateur souhaité dans la liste **Séparateur**.

Pour que UFED Physical Analyzer vérifie automatiquement les images au chargement du projet :

- Sélectionnez **Vérifier automatiquement les images au chargement du projet**.

Pour que UFED Physical Analyzer propose de charger une session à l'ouverture de l'extraction correspondante :

- Sélectionnez **Suggérer la restauration d'un fichier de session à l'ouverture du fichier de vidage correspondant**.

Pour désactiver la mise en évidence des informations :

- Sélectionnez **Désactiver les informations mises en évidence**.

Pour sélectionner toutes les entités dans toutes les vues par défaut :

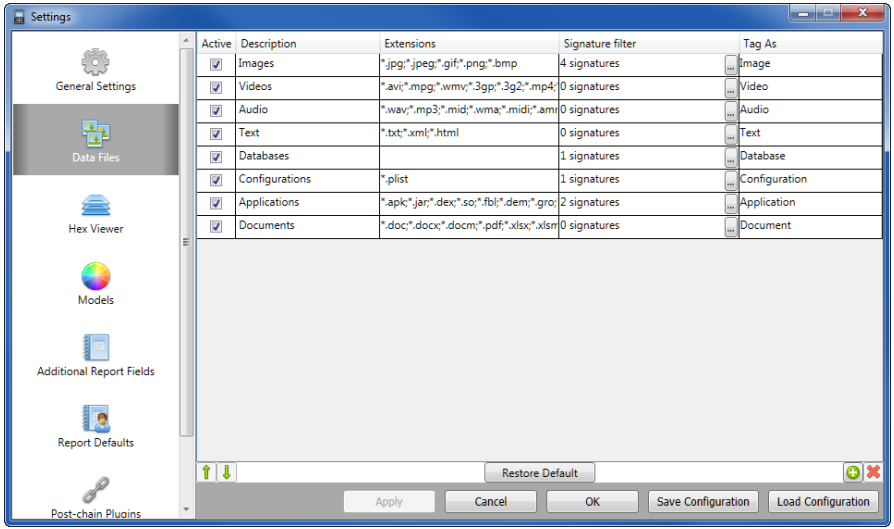
- Sélectionnez **Cocher toutes les entités par défaut**.

  Les entités sélectionnées seront incluses dans les rapports générés.

Pour déterminer le nombre de chiffres requis pour qu'un numéro de téléphone soit unique :

- Dans la zone **Analyse**, sélectionnez le nombre de chiffres souhaités dans le champ **Nombre de chiffres pour qu'un numéro de téléphone soit unique**.

15.2. Fichiers de données



Les paramètres des **Fichiers de données** déterminent les différents groupes de fichiers et de balises dans les éléments d'arborescence **Fichiers de données** et **Balises**, et les types de fichiers filtrés dans chaque groupe.

Chaque enregistrement de fichier de données contient les paramètres suivants :

- **Actif** – indique si le groupe de fichiers de données doit être affiché (coché) ou masqué (décoché) dans l'arborescence de projet.
- **Description** – nom descriptif pour le type de fichiers de données, utilisé comme nom de groupe dans l'élément d'arborescence **Fichiers de données**.
- **Extensions** – extensions de fichier à utiliser pour filtrer les fichiers de données de ce groupe.
- **Filtre signature** – signatures d'en-tête et/ou de pied de page à utiliser pour filtrer les fichiers de données de ce groupe.
- **Baliser comme** – nom de balise à appliquer au fichier de données et utilisé pour répertorier les fichiers dans l'arborescence de projet **Balises**.

15.2.1. Méthodes de filtrage des fichiers de données

Vous pouvez filtrer les groupes en utilisant une ou plusieurs des méthodes suivantes :

- Filtre signature

Un filtre signature est une définition de l'en-tête et/ou du pied de page du fichier à rechercher, permettant de détecter un type de fichier et de l'associer à un groupe de fichiers de données spécifique. L'en-tête et/ou le pied de page peuvent être configurés sur une plage définie à partir du début et de la fin du fichier, respectivement, en utilisant le paramètre de décalage.

Par exemple, une image au format JPEG commence par l'en-tête FF D8 FF et se t
de page FF D9. En saisissant ces informations dans les cha
signature, vous créez une signature qui identifie les images au format JPEG.

- Filtre d'extension

  Un filtre d'extension est une liste d'extensions de fichier courantes associées aux formats de fichiers qui appartiennent au groupe de fichiers de données spécifique.

  Par exemple, il est possible de filtrer les différents formats des fichiers images par les extensions *.jpg, *.jpeg, *.gif, *.png ou *.bmp.

15.2.2. Gérer les paramètres des fichiers de données

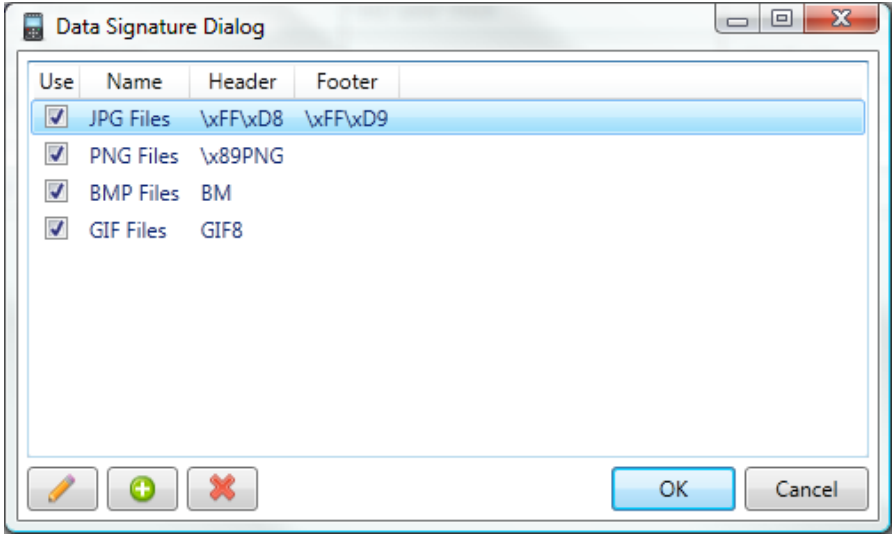
Ajoutez de nouveaux types de fichiers de données, et modifiez et supprimez les types de fichiers de données existants.

15.2.2.1. Ajouter un type de fichiers de données

1) Dans les paramètres **Fichiers de données**, cliquez sur .

   Une nouvelle ligne est ajoutée à la liste.

2) Sélectionnez **Actif** pour afficher le type de données ajouté dans l'élément d'arborescence **Type de données**.
3) Cliquez sur la fenêtre **Description** de la nouvelle ligne, et saisissez une description pour le type de fichiers.
4) Le cas échéant, dans la fenêtre **Extensions**, saisissez les extensions de fichier couramment utilisées par votre type de fichier de données au format ***.xxx**, et séparées par des points-virgules **;**.
5) Le cas échéant, dans la fenêtre **Filtre signature**, cliquez sur et choisissez une des options suivantes :



- Cliquez sur pour ajouter filtre signature qui identifie votre type de fichiers de données.
- Cliquez sur pour modifier un filtre signature existant.
- Cliquez sur pour supprimer un filtre signature.

6) Le cas échéant, dans la fenêtre **Baliser comme**, cliquez sur un nom de balise dans la liste pour le sélectionner.

7) Pour modifier l'ordre des types de fichiers de données, utilisez les flèches .
8) Pour effacer la liste de types de fichiers de données que vous avez ajoutés et conserver uniquement les types par défaut, cliquez sur **Rétablir la liste par défaut**.

15.2.2.2. Modifier un enregistrement de fichier de données existant

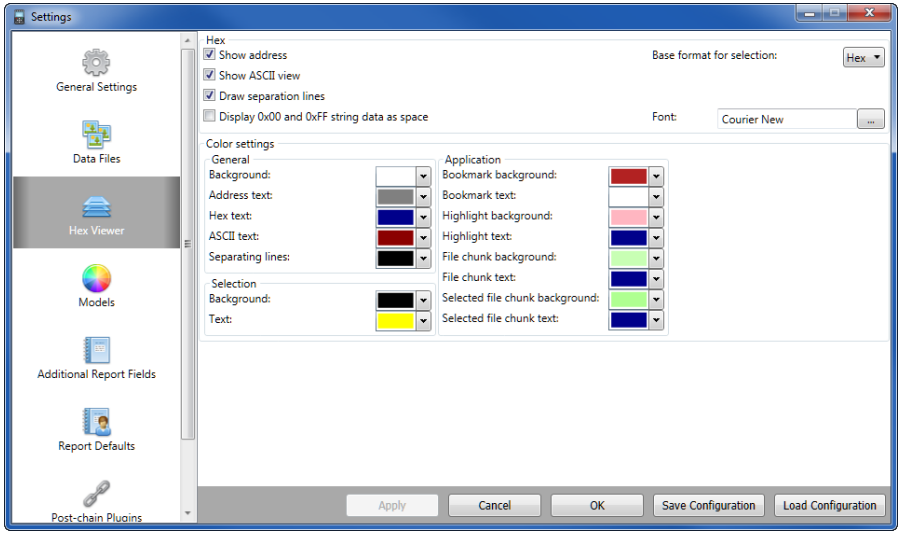
1) Cliquez sur la ligne du type de fichiers de données que vous souhaitez modifier.
2) Double-cliquez sur la colonne et la ligne que vous souhaitez modifier, et mettez à jour les paramètres existants à votre convenance.

15.2.2.3. Supprimer un type de fichier de données

1) Cliquez sur la ligne du type de fichiers de données que vous souhaitez supprimer.
2) Cliquez sur .

15.3. Paramètres de la visionneuse hexadécimale

Les paramètres de la visionneuse hexadécimale vous permettent de contrôler les options d'affichage des extractions hexadécimales afin de les adapter à vos besoins et de les rendre plus lisibles.

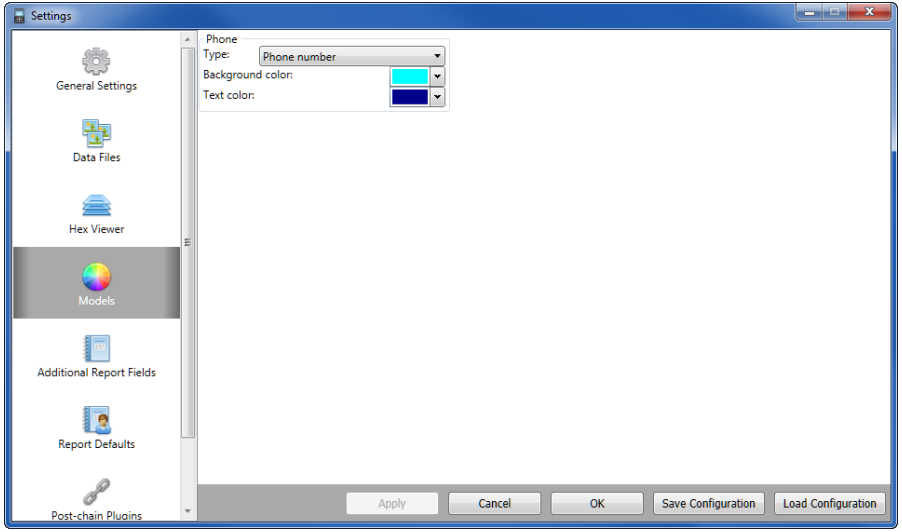


Modifiez les paramètres par défauts suivants de la visionneuse hexadécimale :

- **Afficher l'adresse** – Afficher/Masquer la colonne des numéros de ligne de la visionneuse hexadécimale.
- **Afficher la vue ASCII** – Afficher/Masquer la colonne de la vue ASCII de la visionneuse hexadécimale.
- **Afficher les lignes de séparation** – Afficher/Masquer les lignes de séparation entre les colonnes Adresse, Données hexadécimales et Vue ASCII.
- **Afficher les données de chaîne 0x00 et 0xFF comme un espace** – Les données de chaîne affichent les caractères 0x00 et 0xFF comme un espace au lieu d'un « . ».
- **Format de base pour la sélection** – Format des numéros de ligne (décimal, hexadécimal ou les deux).
- **Police** – Police utilisée pour afficher les informations.
- **Paramètres de couleur** – Définit les couleurs appliquées aux différentes fonctionnalités de la visionneuse hexadécimale.

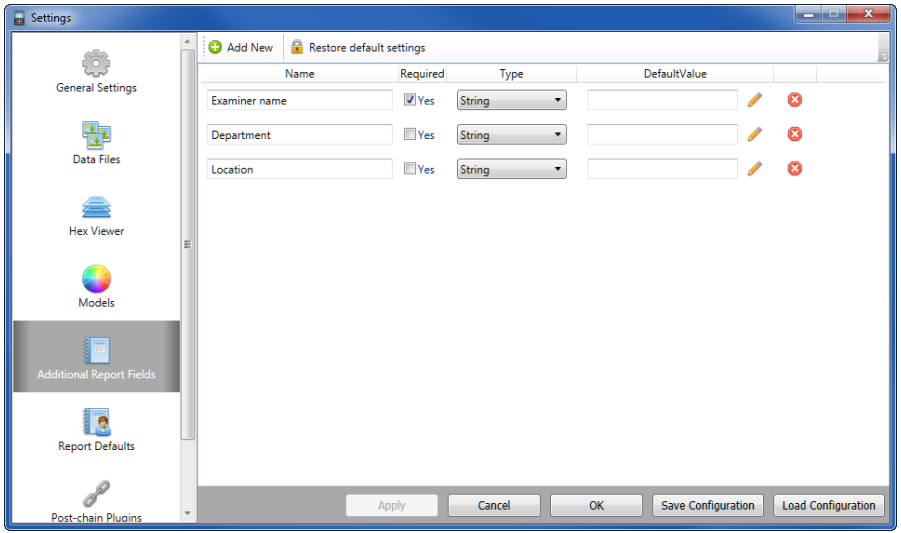
15.4. Paramètres des modèles

Définissez les schémas de couleurs appliqués aux différents types de données de l'appareil.



1) Dans la liste **Type**, sélectionnez le type de données.
2) Dans la liste **Couleur d'arrière-plan**, sélectionnez la couleur d'arrière-plan souhaitée.
3) Dans la liste **Couleur du texte**, sélectionnez la couleur de texte souhaitée.

15.5. Champs de rapport supplémentaires



Ces informations facultatives sont définies par l'utilisateur et présentées au début du rapport. Elles incluent généralement des informations sur le dossier, l'enquêteur et les détails de l'organisation.

Chaque enregistrement d'informations facultatives contient les informations suivantes :

Nom	Nom du champ de rapport.
Obligatoire	Indique que le champ doit être renseigné pour générer le rapport.
Type	Types d'entrée : **Chaîne** ou **Liste**.
Valeur par défaut	Contenu par défaut.

Vous pouvez ajouter des champs de rapport, et modifier et supprimer des champs, à votre convenance.

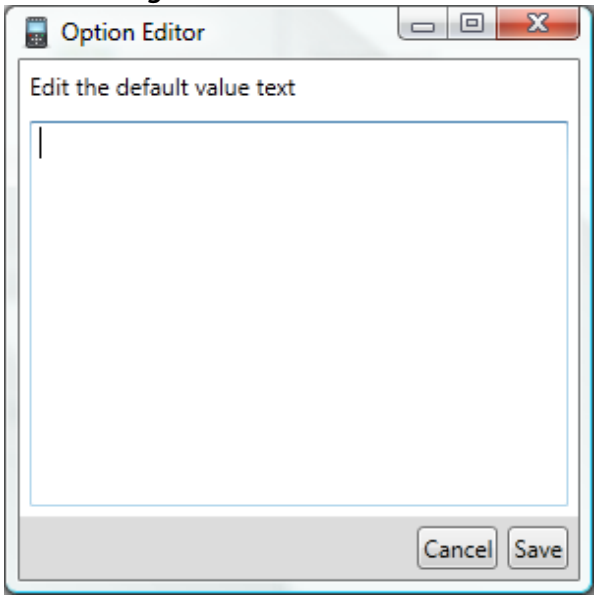
15.5.1. Ajouter un champ de rapport

1) Cliquez sur **Ajouter**.

   Une nouvelle ligne est ajoutée au tableau.

2) Dans la colonne **Nom**, saisissez le nom à afficher.
3) Sélectionnez **Obligatoire** si ce champs doit être rempli pour que l'utilisateur puisse générer le rapport.
4) Dans la liste **Type**, sélectionnez une des options suivantes :
   - **Chaîne** pour les champs de saisie de texte ;
   - **Liste** pour une liste d'options spécifiées.
5) Dans le champ **Valeur par défaut**, définissez le contenu par défaut :

- Pour le type **Chaîne**, saisissez la chaîne par défaut. Pour une chaîne de plusieurs lignes, cliquez sur , saisissez la chaîne par défaut dans l'Éditeur d'option, puis cliquez sur **Enregistrer**.



- Pour le type **Liste**, cliquez sur , saisissez les éléments de la liste, un par ligne, puis cliquez sur **Enregistrer**.

15.5.2. Modifier un champ de rapport

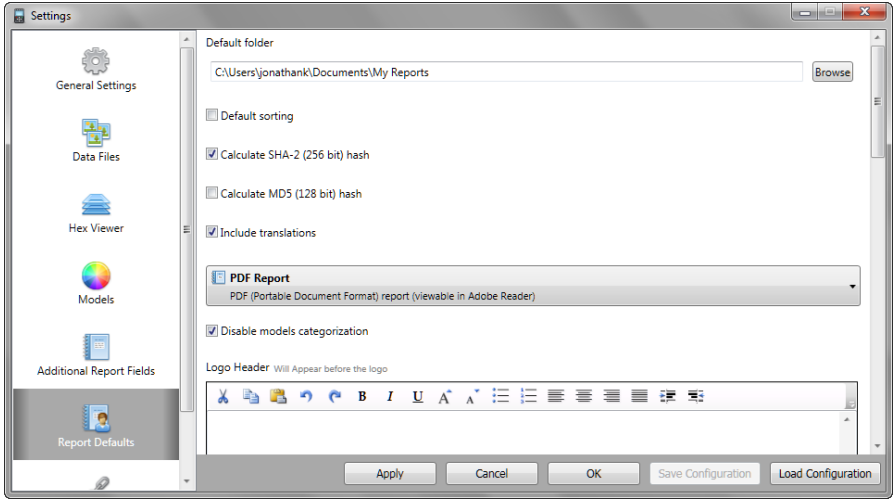
- Pour modifier un champ de rapport, suivez les étapes 2 à 5 de la section ***Ajouter un champ de rapport*** (page ***357***), et modifiez les paramètres à votre convenance.

15.5.3. Supprimer un champ de rapport

- Pour supprimer un champ de rapport, cliquez sur .

15.6. Paramètres par défaut du rapport

Les **Paramètres par défaut du rapport** vous permettent de modifier la présentation du rapport.



REMARQUE : Faites défiler vers le bas pour voir tous les champs.

1) Dans la liste **Type de rapport**, sélectionnez le type de rapport que vous souhaitez modifier.
2) Pour les rapports au format Excel, définissez les options suivantes :
    - **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
    - Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de

données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.

- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Caractère générique pour les caractères non imprimables** – définissez le caractère générique qui remplace les caractères non imprimables.
- **Format du fichier de sortie** – définissez le format de sortie du fichier tableur, au choix :
  * **XLSX** – format de fichier Excel actuel.
  * **XLS** – ancien format de fichier Excel.
  * **ODS** – format de fichier tableau OpenOffice.
- **Rapport Excel compatible avec OpenOffice** – sélectionnez cette option pour vous assurer que le rapport Excel pourra être ouvert sous OpenOffice.
- **Générer les données d'identification du contact** – sélectionnez cette option pour ajouter une feuille au rapport Excel contenant une liste des contacts uniques en fonction du type.

3) Pour les rapports au format HTML, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).

- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.
- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.
- **Diviser le rapport HTML** – chaque section du rapport commence sur une nouvelle page.

4) Pour les rapports au format PDF, définissez les options suivantes :
    - **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
    - Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
    - **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
    - **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
    - **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).

- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.
- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.
- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail.
- **Afficher le corps entier de l'e-mail** – affiche la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.

5) Pour les rapports au format package UFED, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.

- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.
- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions :** Sélectionnez cette option pour inclure le texte traduit dans le rapport.

6) Pour les rapports au format Word, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.

- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.
- **Désactiver la catégorisation des modèles** – sélectionnez cette option pour désactiver la séparation et générer un rapport dans lequel chaque élément de données est généré comme une section unique, sans séparation en sous-catégories. Par défaut, le rapport créé est organisé en catégories, et chaque catégorie du groupe d'éléments de données est générée comme section séparée du rapport. Par exemple, lorsque vous générez un rapport avec des SMS, cochez cette case pour générer les SMS sous forme de liste unique, ou décochez-la pour créer une liste distincte pour chaque catégorie de SMS (reçus, envoyés, brouillons, etc.).
- **En-tête du logo** – saisissez et personnalisez le format du texte qui s'affiche dans l'en-tête du rapport avant le logo.
- **Logo** – cliquez sur **Sélectionner un fichier image** pour ajouter l'image du logo à l'en-tête du rapport. Les formats compatibles sont : BMP, JPG, GIF et PNG.
- **Pied de page du logo** – saisissez et personnalisez le format du texte qui s'affiche dans le pied de page du rapport après le logo.
- **Afficher les totaux pour les éléments exclus du rapport** – ajoute une colonne **Total** au rapport qui affiche le nombre total d'éléments exclus du rapport.

- **Afficher le statut complet des éléments supprimés** – inclut le statut (**Intact**, **Supprimé** ou **Inconnu**) des éléments supprimés dans le rapport généré. Lorsque cette option n'est pas sélectionnée, le statut des éléments supprimés est simplement « Oui », et reste vide pour les autres statuts.
- **Nombre de lignes de l'aperçu d'e-mail** – définit le nombre maximum de lignes affiché dans le rapport pour chaque e-mail. Le rapport inclut des liens vers les fichiers texte contenant la totalité des e-mails.
- **Afficher le corps entier de l'e-mail** – sélectionnez cette option pour afficher la totalité du corps du message.
- **Nombre de messages par conversation instantanée** – définit le nombre maximum de lignes affiché dans le rapport pour chaque conversation instantanée.
- **Afficher tous les messages des conversations instantanées** – affiche dans le rapport la totalité des messages des conversations instantanées.

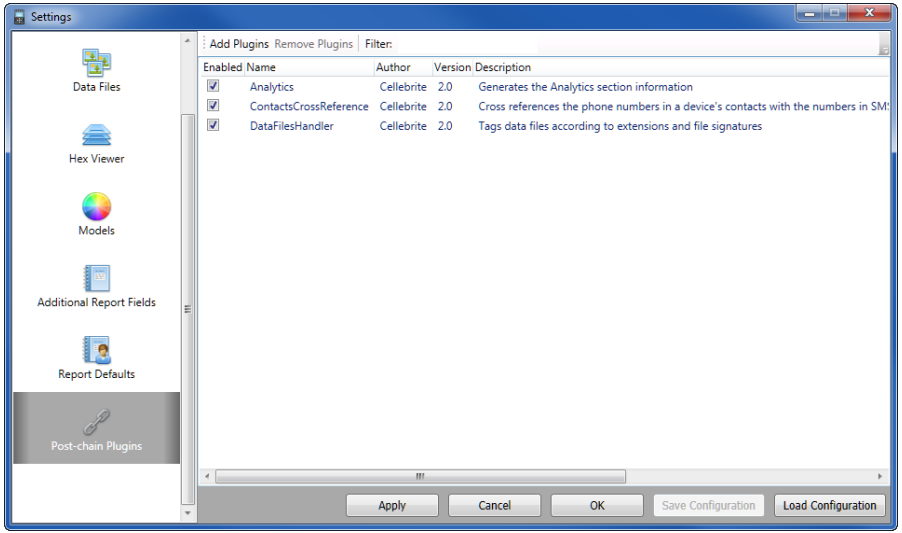
7) Pour les rapports au format XML, définissez les options suivantes :

- **Dossier par défaut** – saisissez le chemin du dossier dans lequel vous souhaitez enregistrer les rapports que vous générez pour ce type de rapport.
- Sélectionnez **Tri par défaut** pour trier les éléments inclus dans le rapport généré en fonction du tri par défaut défini par Cellebrite pour chaque type de fichier analysé et de données, ou désélectionnez **Tri par défaut** pour trier les éléments en fonction du champ de tri sélectionné et de l'ordre de tri (croissant ou décroissant) défini par l'utilisateur dans chaque tableau d'affichage de données.

- **Calculer le hachage SHA-2 (256 bits)** et **Calculer le hachage MD5 (128 bits)** – sélectionnez les clés de hachage MD5 et SHA256 calculées à ajouter à chaque élément des fichiers de données dans le rapport généré. Désactivez ces options pour raccourcir la durée du processus de création du rapport pour les projets de taille importante.
- **Inclure les traductions** – sélectionnez cette option pour inclure le texte traduit dans le rapport.

15.7. Paramètres de plug-in post-chaîne

Ajoutez et supprimez des plug-ins de la liste de plug-ins qui s'exécutent automatiquement lorsque vous ouvrez un projet. Cette fonctionnalité est utile lorsque vous travaillez avec des contraintes temporelles ou avec des fichiers d'extractions volumineux. Ces paramètres vous permettent de décider d'exécuter ou non certains plug-ins.



1) Pour ajouter un plug-in à la liste, cliquez sur **Ajouter des plug-ins** et sélectionnez un plug-in dans la liste.
2) Pour supprimer un plug-in de la liste des plug-ins qui s'exécutent automatiquement lorsque vous ouvrez un projet, décochez la case dans la colonne **Activé**.
3) Pour supprimer un plug-in de la liste, sélectionnez-le et cliquez sur **Supprimer des plug-ins**.
4) Pour filtrer la liste de plug-ins, utilisez le champ **Filtrer**.

REMARQUE : Les paramètres s'appliquent à tous les projets ouverts après la modification dans votre session actuelle. Pour enregistrer votre configuration des paramètres et l'utiliser lors des sessions suivantes, consultez la section ***Enregistrer les paramètres*** (page ***371***).

15.8. Enregistrer les paramètres

Enregistrez vos paramètres pour les réutiliser ultérieurement, ou pour les partager avec un autre utilisateur.

1) Dans la fenêtre Paramètres, cliquez sur **Enregistrer la configuration**.
2) Dans la fenêtre Enregistrer sous, accédez à l'emplacement où vous souhaitez enregistrer votre configuration de paramètres, puis cliquez sur **Enregistrer**.

   Les paramètres sont enregistrés dans un fichier de configuration des paramètres UFED Physical Analyzer (*.cnf).

15.9. Charger des paramètres

Chargez votre configuration de paramètres enregistrée.

1) Dans la fenêtre Paramètres, cliquez sur **Charger la configuration**.
2) Dans la fenêtre Ouvrir, accédez l'enregistrement de votre configuration de paramètres, sélectionnez-la (*.cnf), puis cliquez sur **Ouvrir**.

   Les paramètres sont appliqués dans la fenêtre Paramètres.

15.10. Définir les paramètres du projet

Définissez un fuseau horaire unifié et des informations de dossier pour chaque projet.

15.10.1. Définir un fuseau horaire unifié pour le projet

Au cours de l'extraction, un horodateur est extrait par événement.

Pour les événements sortants, l'horodateur est généralement issu de l'une des sources suivantes :

- Heure de l'appareil définie par l'utilisateur (lorsque l'heure de l'appareil a été définie manuellement par l'utilisateur) : les horodateurs sont affichés sans l'heure locale exacte (UTC).

- Heure de l'appareil définie par le réseau (lorsque l'heure de l'appareil est définie automatiquement par le réseau) : les horodateurs sont affichés avec l'heure locale exacte (UTC).

Pour les événements entrants, l'horodateur est généralement issu de l'heure définie par le réseau (l'horodateur affecté par le réseau). Les horodateurs sont affichés avec l'heure locale exacte (UTC).

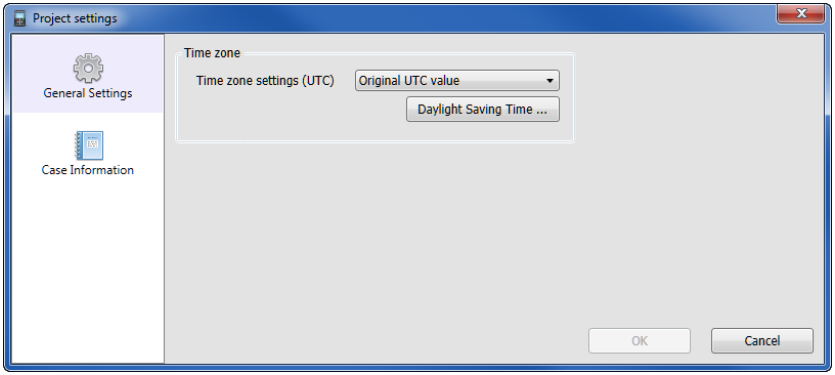
Les horodateurs définis par le réseau dépendent du fuseau horaire dans lequel l'événement s'est produit.

Appliquez un fuseau horaire unifié au projet pour recalculer tous les horodateurs définis par le réseau en fonction du fuseau horaire sélectionné, afin de réunir les événements et de les afficher dans l'ordre dans UFED Physical Analyzer.

Pour appliquer un fuseau horaire unifié au projet :

1) Utilisez une des méthodes suivantes :
    - Dans l'onglet **Résumé d'extraction** du projet, cliquez sur **Paramètres du projet**.

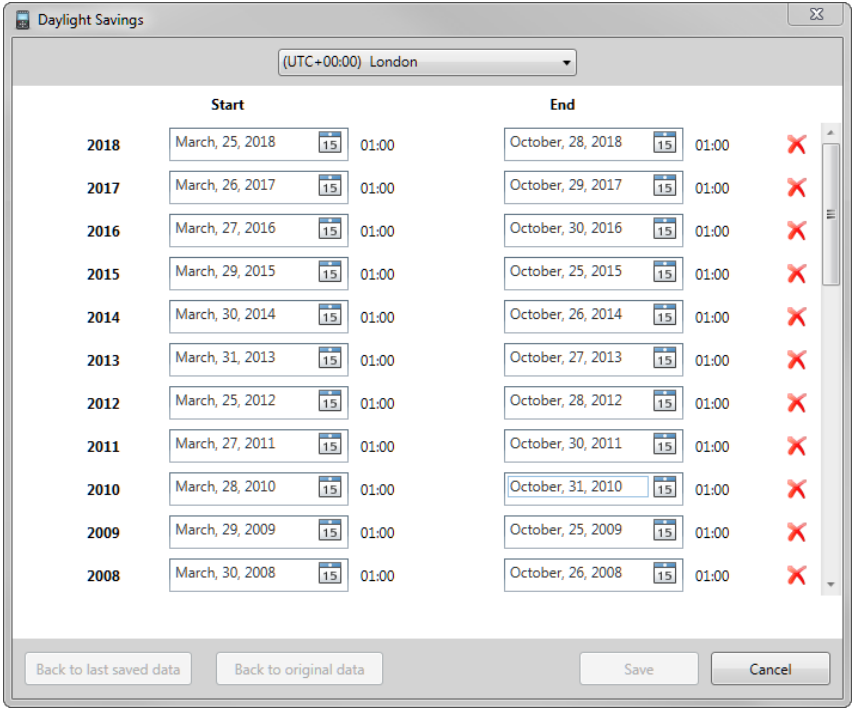
- Cliquez sur .



2) Dans la liste **Paramètres de fuseau horaire (UTC)**, sélectionnez :
   - **Valeur UTC originale** pour afficher les horodateurs tels qu'ils ont été enregistrés (sans unification).
   - Un des fuseaux horaires (**UTC -12:00** à **UTC +13:00**) pour recalculer les horodateurs définis par le réseau en fonction du décalage du fuseau horaire.

   REMARQUE : Les horodateurs définis par l'utilisateur ne sont pas inclus dans ces nouveaux calculs, et sont affichés tels qu'ils ont été enregistrés.

3) Pour modifier les dates de début et de fin de l'heure d'été, cliquez sur **Heure d'été**.


Daylight Savings
(UTC+00:00) London
Start
End
2018 March, 25, 2018 01:00 October, 28, 2018 01:00
2017 March, 26, 2017 01:00 October, 29, 2017 01:00
2016 March, 27, 2016 01:00 October, 30, 2016 01:00
2015 March, 29, 2015 01:00 October, 25, 2015 01:00
2014 March, 30, 2014 01:00 October, 26, 2014 01:00
2013 March, 31, 2013 01:00 October, 27, 2013 01:00
2012 March, 25, 2012 01:00 October, 28, 2012 01:00
2011 March, 27, 2011 01:00 October, 30, 2011 01:00
2010 March, 28, 2010 01:00 October, 31, 2010 01:00
2009 March, 29, 2009 01:00 October, 25, 2009 01:00
2008 March, 30, 2008 01:00 October, 26, 2008 01:00
Back to last saved data
Back to original data
Save
Cancel

a) Pour l'année que vous souhaitez modifier, utilisez le calendrier pour sélectionner les dates de début et de fin, ou modifiez les dates directement. Vous pouvez utiliser le bouton pour supprimer certaines années.

b) Cliquez sur **Revenir aux dernières données enregistrées** pour réinitialiser le tableau à la dernière sauvegarde des données, cliquez sur **Revenir aux données d'origine** pour rétablir les paramètres par défaut du tableau, ou cliquez sur **Enregistrer** pour enregistrer les modifications apportées au tableau.

4) Cliquez sur **OK**.

Le projet est recalculé en fonction du fuseau horaire unifié sélectionné, et le nouveau fuseau horaire est appliqué aux horodateurs définis par le réseau. Les horodateurs des événements affichés dans les fenêtres UFED Physical Analyzer et dans tous les rapports créés ensuite reflètent le fuseau horaire unifié sélectionné.

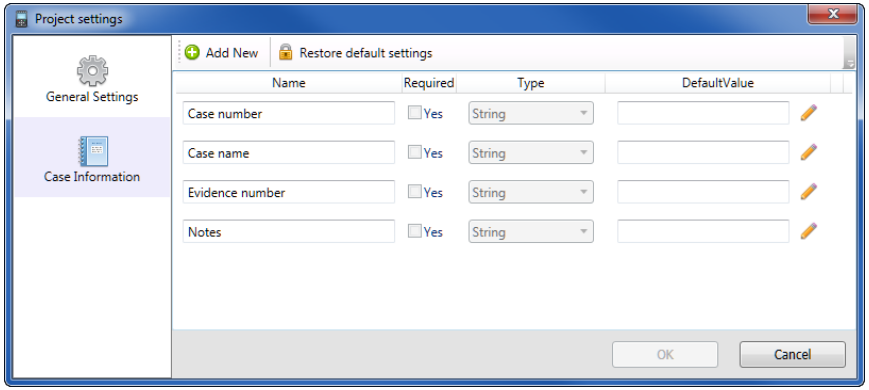
15.10.2. Définir les informations du dossier

Les paramètres d'informations du dossier sont enregistrés avec le projet. Le numéro de dossier apparaît avec les informations d'extraction sur l'onglet Accueil.

1) Utilisez une des méthodes suivantes :

- Dans l'onglet **Résumé d'extraction** du projet, cliquez sur **Paramètres du projet**.
- Cliquez sur .

2) Cliquez sur **Informations du dossier**.



3) Cliquez sur **Ajouter**.

   Certains champs d'informations du dossier sont remplis par défaut.

4) Définissez les paramètres des champs d'information par défauts :

   a) Dans la colonne **Nom**, saisissez les informations correspondantes (par exemple le numéro de dossier, le nom ou des remarques).

   b) Sélectionnez **Obligatoire** si ce champ doit être rempli.

c) Dans la liste **Type**, sélectionnez une des options suivantes :

- **Chaîne** pour les champs de saisie de texte ;
- **Liste** pour une liste d'options spécifiées.

d) Dans le champ **Valeur par défaut**, définissez le contenu par défaut :

- Pour le type **Chaîne**, saisissez la chaîne par défaut. Pour une chaîne de plusieurs lignes, cliquez sur , saisissez la chaîne par défaut dans l'Éditeur d'option, puis cliquez sur **OK**.
- Pour le type **Liste**, cliquez sur , saisissez les éléments de la liste, un par ligne, puis cliquez sur **OK**.

5) Pour ajouter des champs d'information supplémentaires, cliquez sur **Ajouter**, puis répétez l'étape 3.
6) Pour supprimer les saisies personnalisées, cliquez sur .
7) Pour rétablir les paramètres par défaut, cliquez sur **Rétablir les paramètres par défaut**.

Chapitre 16 : **Références**

16.1. Menu Fichier

Ouvrir	Ouvre un fichier pour l'analyser avec le processus d'analyse standard.
Ouvrir (avancé)	Ouvre un fichier pour l'analyser avec le processus d'analyse avancé. Consultez la section ***Ouvrir une extraction en mode avancé*** (page ***44***).
Récent	Affiche une liste des projets récents.
Fermer	Ferme le projet actif.
Enregistrer votre session de projet	Enregistre les informations du projet actif générées par l'utilisateur dans un fichier de session Physical Analyzer (*.pas). Consultez la section ***Enregistrer une session de projet*** (page ***70***).
Charger une session de projet	Charge un fichier de session Physical Analyzer (*.pas) dans un projet ouvert dans l'arborescence de projet.
Fermer	Ferme UFED Physical Analyzer et toutes les sessions actives.

16.2. Menu Vue

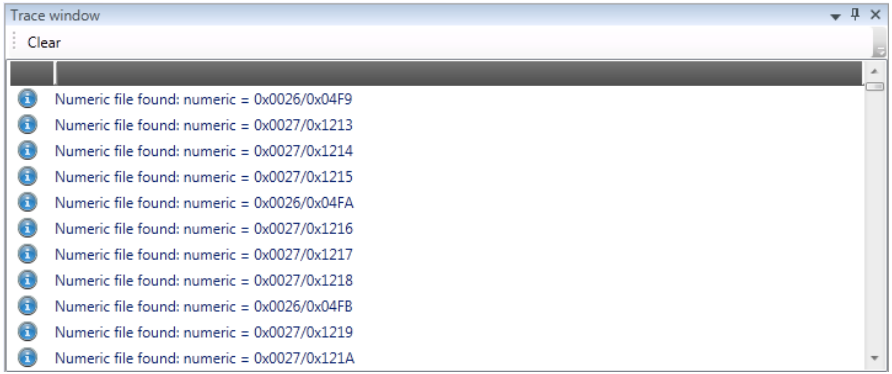
Afficher l'écran d'accueil	Affiche l'onglet **Accueil**. Consultez la section *Onglet Accueil* (page *92*).
Fenêtre Trace	Affiche/Masque la fenêtre Trace en bas de la zone d'affichage des données.

16.2.1. Afficher la fenêtre Trace

Affiche la fenêtre Trace en bas de la zone d'affichage des données, pour voir un journal des actions exécutées au cours de votre session par vous ou UFED Physical Analyzer, par exemple l'activation d'un plug-in.

1) Dans le menu **Vue**, sélectionnez **Fenêtre Trace**.

   La fenêtre Trace s'affiche sous la zone d'affichage des données.


Trace window
Clear
Numeric file found: numeric = 0x0026/0x04F9
Numeric file found: numeric = 0x0027/0x1213
Numeric file found: numeric = 0x0027/0x1214
Numeric file found: numeric = 0x0027/0x1215
Numeric file found: numeric = 0x0026/0x04FA
Numeric file found: numeric = 0x0027/0x1216
Numeric file found: numeric = 0x0027/0x1217
Numeric file found: numeric = 0x0027/0x1218
Numeric file found: numeric = 0x0026/0x04FB
Numeric file found: numeric = 0x0027/0x1219
Numeric file found: numeric = 0x0027/0x121A

2) Pour effacer le journal dans la fenêtre Trace, cliquez sur **Effacer**.
3) Pour fermer la fenêtre Trace, cliquez sur .

La fenêtre Trace peut être masquée ou affichée.

- Pour maintenir ouverte la fenêtre Trace, cliquez sur .
- Pour ne plus maintenir ouverte la fenêtre Trace, cliquez sur .
- Pour afficher la fenêtre Trace lorsqu'elle est masquée, sélectionnez-la ou passez avec le curseur de la souris sur l'onglet.

16.3. Menu Outils

Lire des données depuis UFED	Permet d'extraire des données directement sur l'ordinateur.
Vidage du système de fichiers	Exporte et enregistre le système de fichiers analysé vers les fichiers et dossiers réels dans une structure de répertoire. Consultez la section ***Exporter le système de fichiers*** (page ***340***).
Reconstituer des images	Ouvre la fenêtre Reconstituer des images, qui permet de rechercher des images. Consultez la section ***Reconstituer des images*** (page ***239***)
Reconstituer des chaînes	Ouvre la fenêtre Reconstituer des chaînes, qui permet de rechercher des chaînes.
Éditeur de liste de surveillance	Ouvre la fenêtre Éditeur de liste de surveillance, qui permet de créer, gérer et exécuter vos listes de surveillance. Consultez la section ***Travailler avec les listes de surveillance*** (page ***132***).
Scanner anti-malware	Ouvre le sous-menu Scanner anti-malware, qui permet d'exécuter la détection de malware sur votre extraction, et de mettre à jour la base de données de signature. Consultez la section ***Rechercher les malware*** (page ***177***).

Traduction	Télécharge le package de traduction depuis Internet, installe ce package depuis un fichier ou affiche les langues prises en charge. Consultez la section ***Traduction de données décodées*** (page ***159***).
Ouvrir dans UFED Link Analysis	Ouvre ce projet Physical Analyzer dans UFED Link Analysis.
TomTom	Ouvre le sous-menu TomTom, qui permet d'exporter le fichier d'extraction TomTom et d'importer le fichier XML qui vous est renvoyé. Consultez la section ***Travailler avec TomTom*** (page ***235***).
Paramètres	Accède à la fenêtre Paramètres de l'application. Consultez la section ***Paramètres*** (page ***343***).
Paramètres du projet	Définissez un fuseau horaire unifié et des informations de dossier pour chaque projet. Consultez la section ***Définir les paramètres du projet*** (page ***372***).

16.4. Menu Extraction

Extraction d'appareil iOS

Lance l'extraction d'appareil iOS pour effectuer des extractions d'appareils iOS. Consultez la section ***Extraction d'appareils iOS*** (page ***199***).

Extraire GPS/Appareil de stockage de masse

Lit et enregistre les données d'appareils GPS et de stockage de masse connectés au poste de travail par un câble USB. Consultez la section ***Lire des données depuis un appareil GPS ou de stockage de masse*** (page ***230***).

16.5. Menu Python

Shell Python

Ouvre la fenêtre Shell Python qui permet d'effectuer une analyse personnalisée en utilisant les commandes Python. Consultez la section ***Utiliser le shell Python*** (page ***339***). Pour en savoir plus sur l'utilisation des commandes du shell Python pour l'analyse personnalisée, consultez le « Guide d'écriture de script Python », disponible dans le menu **Aide**.

Exécuter le script

Exécute un script Python pré-écrit (fichier *.py).

Exécuter le script (débogage activé)

Vous permet d'exécuter un script Python pré-écrit (fichier *.py) en mode débogage.

16.6. Menu Plug-ins

Ajouter/Supprimer des plug-ins — Affiche une liste des plug-ins préinstallés pour activer la gestion des plug-ins déjà installés. Consultez la section ***Gérer les plug-ins*** (page ***335***)

Exécuter le plug-in — Permet à l'utilisateur de sélectionner un plug-in spécifique et de l'exécuter. Consultez la section ***Exécuter un plug-in spécifique*** (page ***337***).

Gestionnaire de chaînes — Affiche la fenêtre Gestionnaire de chaîne, qui permet de gérer et de créer des chaînes de traitement de l'appareil. Consultez la section ***Gérer les chaînes*** (page ***317***)

16.7. Menu Rapport

Générer un rapport — Génère un résumé du rapport contenant toutes les informations trouvées lors du processus d'analyse. Consultez la section Générer un rapport.

16.8. Menu Aide

Applications prises en charge	Répertorie les applications prises en charge et les versions vérifiées pour les appareils Android et iOS.
Manuel	Ouvre le manuel de l'utilisateur au format PDF.
Guide d'écriture de script du shell Python	Ouvre le Guide d'écriture de script Python au format PDF.
Activer les cartes Bing en ligne	Active les cartes Bing pour vous permettre d'afficher les emplacements sur une carte. Un accès à Internet et une licence UFED Physical Analyzer valide sont nécessaires.
Lancer la démonstration UFED Link Analysis	Lance l'application UFED Link Analysis.
Afficher les détails de licence	Affiche les informations de licence logicielle ou matérielle (dongle), et vous permet : • D'activer ou de charger une nouvelle licence (logicielle ou dongle) ; • D'afficher des informations sur les précédents dongles qui ont été connectés à ce poste de travail ; • De désactiver une licence logicielle ; • De contacter l'assistance et le service des ventes Cellebrite par e-mail.
Zipper les fichiers journaux	Zippe les fichiers journaux et ouvre le dossier dans lequel les fichiers zippés sont enregistrés.

Zipper les fichiers journaux avec informations système	Zippe les fichiers journaux et inclut des informations détaillées concernant le système d'exploitation, les pilotes, les données d'application, les journaux d'événements, etc. Ces informations peuvent être utilisées pour analyser les cas de rapport.
À propos de UFED Physical Analyzer	Fournir des informations sur la version installée de UFED Physical Analyzer.

A

À propos des données de localisation • 80, 146, 231

Activation à l'aide d'une licence logicielle • 35, 37

Activer UFED Physical Analyzer • 27

Afficher la fenêtre Trace • 376

Afficher les données de localisation sur BING • 149

Afficher les fichiers image • 95, 114, 239

Afficher les informations des données hexadécimales • 305

Ajouter un champ de rapport • 353, 355

Ajouter un signet • 300

Ajouter un type de fichiers de données • 345

Ajouter un vidage binaire • 55, 61, 63

Ajouter un vidage de système de fichiers • 56, 61, 63

Analyse de données • 14

Arborescence de projet • 74, 93, 143

Associer des appareils à une chaîne • 320

Avis juridiques • 3

C

capture d'écran • 309

Capture d'image • 309

Champs de rapport supplémentaires • 187, 352

Charger des paramètres • 367

Charger une session de projet • 70

Clé de licence (dongle) • 28

Clé réseau • 33

Commencer avec un nouveau projet • 59, 61

Commencer par la sélection de l'appareil • 59

Conditions préalables • 195

Configuration requise • 18

Construire une chaîne • 315

Création d'un rapport – Assistant de création de rapports • 183

Créer un nouveau signet d'entité • 144

Créer une liste de surveillance • 130, 141, 142

D

Décodage avancé • 49, 313

Décoder des données brutes • 303

Définir la chaîne d'appareils par défaut • 323

Définir les informations du dossier • 187, 371

Définir les paramètres du projet • 87, 367, 379

Définir un fuseau horaire unifié pour le projet • 367

Démonstration de Link Analysis • 40

Déplacer UFED Physical Analyzer vers un autre PC à l'aide d'une licence logicielle • 35

Désactivation des licences de la version 2 • 35

Désactivation des licences de la version 5 • 36

Dissocier des appareils d'une chaîne • 325

E

Effectuer des extractions • 195

Effectuer une extraction numérique avancée • 212

Effectuer une extraction physique • 196

Effectuer une extraction physique d'appareils cryptés • 205, 206

Effectuer une extraction physique d'appareils iOS non cryptés • 197, 207, 209

Enregistrement d'un fichier .ufd • 69

Enregistrer les paramètres • 70, 339, 366

Enregistrer une chaîne personnalisée • 54

Enregistrer une session de projet • 69, 375

Espace libre • 12

Exécuter un plug-in spécifique • 333, 337, 381

Exécuter une liste de surveillance • 140

Exécuter une liste de surveillance sur des projets spécifiques • 141

Exécuter une liste de surveillance sur votre projet en cours • 142

Exporter le système de fichiers • 336, 378

Exporter un fichier TomTom • 232

Exporter une liste de surveillance • 138

Extraction d'appareils iOS • 195, 379

Extraction de données d'un appareil avec mot de passe complexe • 209

Extraction de données d'un appareil avec mot de passe simple • 207

Extraction du GPS ou des appareils de stockage de masse • 223

Extraction physique • 12

F

Fermer UFED Physical Analyzer • 71

Fermer un projet • 71

Fichier ufdx • 310, 312

Fichiers de données • 93, 343

G

Gérer les chaînes • 54, 313, 381

Gérer les chaînes d'appareils • 320

Gérer les paramètres des fichiers de données • 81, 345

Gérer les plug-ins • 331, 381

H

Heure d'été • 341

I

Importer un fichier TomTom • 233

Importer une liste de surveillance • 135

Indicateurs et fenêtres d'informations • 152

Informations sur les signets (signets d'entités) • 85, 143

Installation du logiciel • 19

Installation et activation • 17

Installer UFED Physical Analyzer • 18, 20

Introduction • 11

J

JTAG • 63

L

Lancer UFED Physical Analyzer • 40

Licence logicielle • 30

Lire des données depuis un appareil GPS ou de stockage de masse • 226, 231, 379

Lire des fichiers vidéo ou audio • 116

Localisation des appareils • 146

Localisation et analyse des informations • 117

Localiser des types de données spécifiques dans les données hexadécimales • 306

Localiser une liste de surveillance • 143

M

Menu Aide • 382

Menu Extraction • 379

Menu Fichier • 375

Menu Outils • 378

Menu Plug-ins • 381

Menu Python • 380

Menu Rapport • 381

Menu Vue • 376

Méthodes de filtrage des fichiers de données • 344

Mettre à jour la base de données de signature (en ligne) • 173, 174

Mettre à jour la base de données de signature depuis un fichier (hors connexion) • 173, 176

Mise en route • 39

Modifier la chaîne actuelle • 51, 61, 63

Modifier la chaîne de décodage • 49

Modifier un champ de rapport • 355

Modifier un enregistrement de fichier de données existant • 348

Modifier un signet • 303

Modifier un signet d'entité • 145

Modifier une chaîne existante • 317

Modifier une liste de surveillance • 135

N

Notification de nouvelle version • 27

O

Obtenir une copie de UFED Physical Analyzer • 19

Onglet Accueil • 90, 376

Onglet Infos fichier • 113

Onglet Résumé d'extraction • 92

Onglets de données • 94

Ouverture avancée d'un fichier d'extraction non-UFED • 57

Ouverture avancée d'un fichier d'extraction UFED • 44

Ouvrir une extraction en mode avancé • 41, 42, 44, 375

Ouvrir une extraction pour analyse • 41

P

Paramètres • 339, 379

Paramètres avancés • 231

Paramètres de la visionneuse hexadécimale • 250, 255, 261, 266, 271, 278, 284, 290, 295, 349

Paramètres de plug-in post-chaîne • 365

Paramètres des modèles • 351

Paramètres généraux • 340

Paramètres par défaut du rapport • 187, 355

Parcourir le système de fichiers • 122

Parcourir l'extraction hexadécimale • 298

Permettre la connectivité avec Windows Vista • 19, 37

Plug-in de reconstitution de mot de passe de déverrouillage Android • 337

Plug-ins • 49, 330

Présentation • 11

R

Raccourcis • 72

Rechercher des chaînes • 247, 248

Rechercher des chaînes de texte de SMS • 248, 281

Rechercher des codes et des mots de passe • 248, 293

Rechercher des dates • 247, 258

Rechercher des expressions régulières (GREP) • 248, 275

Rechercher des informations dans les données hexadécimales et dans les données décodées • 246

Rechercher des informations dans tous les projets ouverts • 121

Rechercher des informations dans un onglet de données • 117

Rechercher des numéros SIM ICCID • 247, 264

Rechercher des numéros SMS • 247, 269

Rechercher des octets • 247, 253

Rechercher des schémas • 248, 287

Rechercher les images reconstituées • 236

Rechercher les malware • 86, 173, 378

Reconstituer des images • 82, 235, 378

Récupération des adresses • 153

Références • 375

S

Sélectionner des langues • 156

Sélectionner une chaîne différente • 50, 61, 62

S'orienter dans l'espace de travail • 40, 73

Spécifier un appareil différent • 47, 61, 62

Supprimer un champ de rapport • 355

Supprimer un signet • 303

Supprimer un signet d'entité • 146

Supprimer un type de fichier de données • 348

Supprimer une chaîne • 326

Supprimer une liste de surveillance • 140

T

Traduction de données décodées • 155

Travailler avec l'analyse de projet • 169

Travailler avec les données hexadécimales • 123, 243

Travailler avec les images reconstituées • 239

Travailler avec les listes de surveillance • 84, 130, 378

Travailler avec les signets • 109, 245, 300

Travailler avec TomTom • 231, 379

Travailler dans la zone Arborescence de projet • 87

Travailler dans les onglets de données • 95

Travailler dans l'onglet Mises en évidence • 109, 112, 245

Travailler dans l'onglet Valeurs • 109, 110, 245

U

Utiliser le filtre avancé • 120

Utiliser le filtre rapide • 117

Utiliser le plug-in de reconstitution de schéma de déverrouillage Android • 336

Utiliser le shell Python • 335, 380

Utiliser un décalage pour accéder directement à un emplacement différent dans le fichier • 299

V

Vérifier les valeurs de hachage • 93, 240

Vue base de données • 104

Vue Chronologie • 124

Vue Conversation • 127

Vue dossier • 102

Vue hexadécimale • 106, 123, 245

Vue tableau pour les données analysées • 101

Vue tableau pour les fichiers de données • 99

Vue texte • 98

Z

Zone d'affichage de données • 88